

2.1 TREND MICRO™ Security

Administratorhandbuch

Für große und mittlere Unternehmen

für MAC







Trend Micro Incorporated behält sich das Recht vor, ohne Vorankündigung Änderungen an diesem Dokument und den hierin beschriebenen Produkten vorzunehmen. Lesen Sie vor der Installation und Verwendung der Software die Readme-Dateien, die Anmerkungen zu dieser Version und die neueste Version der zugehörigen Benutzerdokumentation auf der Homepage von Trend Micro unter:

http://docs.trendmicro.com/de-de/enterprise/trend-micro-security-(for-mac).aspx

Dokument-Nr.: TSGM26484/140925

Release-Datum: Oktober 2014

In der Benutzerdokumentation für Trend Micro Security (für Mac) werden die wesentlichen Funktionen der Software und Installationsanweisungen für Ihre Produktionsumgebung erläutert. Lesen Sie die Dokumentation vor der Installation und Verwendung der Software aufmerksam durch.

Ausführliche Informationen über die Verwendung bestimmter Funktionen der Software finden Sie in der Online-Hilfe und der Knowledge Base auf der Website von Trend Micro.

Das Trend Micro Team ist stets bemüht, die Dokumentationen zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder anderen Dokumenten von Trend Micro wenden Sie sich bitte an docs@trendmicro.com.

Bewerten Sie diese Dokumentation auf der folgenden Seite:

http://www.trendmicro.com/download/documentation/rating.asp



Inhaltsverzeichnis

Vorwort

Kapitel 1: Einführung in Trend Micro Security (für Mac)

Kapitel 2: Server installieren

Kapitel 3: Erste Schritte

Kapitel 4: Agent installieren

Kapitel 5: Den Schutz auf dem neuesten Stand halten

Kapitel 6: Mac-Computer vor Sicherheitsrisiken schützen

Kapitel 7: Mac-Computer vor webbasierten Angriffen schützen

Kapitel 8: Server und Agents verwalten

Kapitel 9: Hilfe anzeigen

Anhang A: IPv6-Unterstützung in Trend Micro Security (für Mac)

Anhang B: Produktterminologie und -begriffe

Stichwortverzeichnis



Vorwort

Vorwort

Willkommen beim Trend Micro Security (für Mac) **Administratorenhandbuch**. Dieses Dokument enthält die Installationsanleitung für Trend Micro Security (für Mac) Server und Agents sowie Informationen über die ersten Schritte und die Verwaltung von Server und Agents.

Trend Micro Security (für Mac) Dokumentation

Die Dokumentation zu Trend Micro Security (für Mac) umfasst Folgendes:

Dokumentation	Beschreibung
Administratorhandbuch	Ein PDF-Dokument mit Installationsanleitungen für Trend Micro Security (für Mac) Server und Agents sowie Informationen über die ersten Schritte und die Verwaltung von Server und Agents.
Hilfe	HTML-Dateien mit praktischen Tipps, Benutzerhinweisen und Angaben zu den einzelnen Feldern
Readme-Datei	Enthält eine Liste bekannter Probleme und grundlegende Installationshinweise. Sie kann auch neueste Produktinformationen enthalten, die in anderen Dokumenten nicht zur Verfügung stehen.
Knowledge Base	Eine Online-Datenbank mit Informationen zur Problemlösung und Fehlerbehebung. Sie enthält die aktuellsten Hinweise zu bekannten Softwareproblemen. Die Knowledge Base finden Sie im Internet unter folgender Adresse: http://esupport.trendmicro.com

Die Produktdokumentation können Sie unter den folgenden Adresse anzeigen und herunterladen:

http://docs.trendmicro.com/de-de/enterprise/trend-micro-security-(for-mac).aspx

Zielgruppe

Die Dokumentation zu Trend Micro Security (für Mac) richtet sich an folgende Benutzer:

- **Trend Micro Security (für Mac) Administratoren**: Verantwortlich für die Verwaltung von Trend Micro Security (für Mac), einschließlich Installation und Verwaltung von Server und Agents. Es wird davon ausgegangen, dass diese Benutzer über umfassende Kenntnisse über Netzwerke und Server-Verwaltung verfügen.

- **Endbenutzer**: Benutzer, die den Trend Micro Security (für Mac) Agent auf einem Mac-Computer installiert haben. Die Computerkenntnisse dieser Benutzergruppe reichen vom Anfänger bis zum erfahrenen Anwender.

Textkonventionen

Damit Sie Informationen leicht finden und einordnen können, kommen in der Dokumentation zu Trend Micro Security (für Mac) folgende Konventionen zur Anwendung:

TABELLE 1. Textkonventionen

KONVENTION	BESCHREIBUNG
NUR GROSSBUCHSTABEN	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Befehlsschaltflächen, Registerkarten, Optionen und Tasks
Kursivdruck	Referenzen zu anderen Dokumenten oder neuen technischen Komponenten
<Text>	Text in spitzen Klammern soll durch Benutzerangaben ersetzt werden. Beispiel: `C:\Programme\<Dateiname>` durch `C:\Programme\beispiel.jpg`.
Hinweis	Enthält Konfigurationshinweise oder -empfehlungen
Tipp	Enthält Angaben zu bewährten Methoden und Trend Micro Empfehlungen
Warnung!	Enthält Warnungen zu Vorgängen, die Computern im Netzwerk schaden können

Begriff

Die folgende Tabelle enthält offizielle Begriffe, die in der gesamten Trend Micro Security (für Mac) Dokumentation verwendet werden:

Begriff	Beschreibung
Agent	Trend Micro Security (für Mac) Agent-Programm, das auf einem Mac-Computer installiert ist
Endpunkt	Mac-Computer, auf dem der Agent installiert ist
Agent-Benutzer (oder Benutzer)	Person, die den Agent auf dem Mac-Computer verwaltet
Server	Trend Micro Security (für Mac) Server-Programm
Server-Computer	Computer, auf dem der Trend Micro Security (für Mac) Server installiert ist
Administrator (oder Trend Micro Security (für Mac) Administrator)	Person, die den Trend Micro Security (für Mac) Server verwaltet
Konsole	Benutzerschnittstelle zur Konfiguration und Verwaltung der Trend Micro Security (für Mac) Server- und Agent-Einstellungen Die Konsole für das Serverprogramm wird ‚Webkonsole' genannt, die Konsole für den Agent heißt ‚Agent-Konsole'.
Sicherheitsrisiko	Oberbegriff für Viren, Malware, Spyware/Grayware und Internet-Bedrohungen
Produktdienst	Trend Micro Security (für Mac) Dienst, der von der Microsoft Management Console (MMC) aus verwaltet wird
Komponenten	Suchen und entdecken Sicherheitsrisiken und führen Aktionen gegen sie durch.

Begriff	Beschreibung
`Agent-Installationsordner`	Ordner auf dem Mac-Computer, der die Programmdateien des Trend Micro Security (für Mac) Agents enthält `/Library/Application Support/TrendMicro`
`Server-Installationsordner`	Ordner auf dem Server-Computer, der die Programmdateien des Trend Micro Security (für Mac) Servers enthält Nach der Installation von Trend Micro Security (für Mac) Server wird der Ordner im gleichen Verzeichnis wie der Worry-Free Business Security Server-Ordner erstellt. Wenn Sie die Standardeinstellungen bei der Installation von Worry-Free Business Security übernehmen, ist der Server-Installationsordner einer der Folgenden: • `C:\Programme\Trend Micro\Security Server\Addon\TMSM` • `C:\Programme (x86)\Trend Micro\Security Server\Addon\TMSM`
Dualstapel	Entität, die sowohl IPv4- als auch IPv6-Adressen hat. Zum Beispiel: • Ein Dualstapel-Endpunkt ist ein Mac-Computer mit IPv4- und IPv6-Adressen. • Ein Dualstapel-Agent ist ein Agent, der auf einem Dualstapel-Endpunkt installiert ist. • Ein Dualstapel-Proxy-Server wie beispielsweise DeleGate kann IPv4- in IPv6-Adressen konvertieren und umgekehrt.
Reine IPv4	Entität, die nur eine IPv4-Adresse hat
Reine IPv6	Entität, die nur eine IPv6-Adresse hat



Kapitel 1

Einführung in Trend Micro Security (für Mac)

Dieses Kapitel stellt eine Einführung in Trend Micro™ Security (für Mac) dar und gibt eine Übersicht über die Funktionen und Fähigkeiten.

Informationen zu Trend Micro Security (für Mac)

Trend Micro™ Security (für Mac) bietet modernsten Schutz für Endpunkte vor Sicherheitsrisiken, kombinierten Bedrohungen und plattformunabhängigen webbasierten Angriffen.

Trend Micro Security (für Mac) Server ist ein Plug-in-Programm, das in Trend Micro Produkte wie OfficeScan und Worry-free Business Security integriert und über das Plug-in Manager-Framework installiert wird. Trend Micro Security (für Mac) Server stellt Agents für Mac-Computer bereit.

Wichtigste Funktionen und Vorteile

Trend Micro Security (für Mac) bietet die folgenden Funktionen und Vorteile:

- **Schutz vor Sicherheitsrisiken**

  Trend Micro Security (für Mac) schützt Mac-Computer vor Sicherheitsrisiken, indem Dateien durchsucht werden und dann eine spezifische Aktion für jedes entdeckte Sicherheitsrisiko durchgeführt wird. Wird eine große Anzahl von Sicherheitsrisiken innerhalb kurzer Zeit erkannt, deutet dies auf einen Virenausbruch hin. Trend Micro Security (für Mac) benachrichtigt Sie über jeden Ausbruch, sodass Sie sofort entsprechende Maßnahmen ergreifen können, wie z. B. die betroffenen Computer von der Schadsoftware zu befreien und sie so lange zu isolieren, bis keine Bedrohung mehr von ihnen ausgeht.

- **Web Reputation**

  Web Reputation schützt Mac-Computer innerhalb oder außerhalb des Unternehmensnetzwerks proaktiv vor bösartigen und potenziell gefährlichen Websites. Web Reputation durchbricht die Infektionskette und verhindert den Download bösartigen Codes.

- **Zentrale Verwaltung**

  Eine webbasierte Management-Konsole ermöglicht dem Administrator einen übersichtlichen Zugriff auf alle Agents im Netzwerk. Über die Webkonsole wird

außerdem die automatische Verteilung von Sicherheitsrichtlinien, Pattern-Dateien und Software-Updates auf allen Agents koordiniert. Der Administrator kann das Netzwerk remote verwalten und Einstellungen für einzelne Agents Clients oder Agent-Gruppen vornehmen.

Neu in dieser Version

Trend Micro Security (für Mac) bietet die folgenden neuen Funktionen und Verbesserungen:

FUNKTION/VERBESSERUNG	DETAILS
Verbesserte Suchleistung und -funktionalität	• Der Zwischenspeicher der On-Demand-Suche verbessert die Leistung bei der Suche und reduziert die dafür erforderliche Zeit, indem bereits durchsuchte bedrohungsfreie Dateien übersprungen werden. • Mit Hilfe von Platzhalterzeichen können schnell und einfach Ordner für den Suchausschluss festgelegt werden. • Benutzern kann gestattet werden, die zeitgesteuerte Suche zu verschieben, zu überspringen oder abzubrechen.
Einfacheres Aktivierungsverfahren	Der Trend Micro Security (für Mac) Server wird bei der Installation des Worry-Free Business Security 9.0 Plug-in Manager automatisch aktiviert.
Worry-Free Business Security Standard-Support	Worry-Free Business Security Standard unterstützt nun die Installation von Trend Micro Security (für Mac) Servern.
Smart Protection für Web Reputation	Agents senden Web-Reputation-Abfragen an das Smart Protection Network, um die Sicherheit von Websites zu ermitteln.
Verbesserungen bei Aktualisierungen	Agents können Aktualisierungen anhand von Zeitplänen ausführen und vom Trend Micro ActiveUpdate Server beziehen, wenn der Trend Micro Security (für Mac) Server nicht verfügbar sein sollte.

FUNKTION/VERBESSERUNG	DETAILS
Unterstützung für IPv6	Trend Micro Security (für Mac) Server und Agents können nun auch auf IPv6-Computern installiert werden.
Unterstützung für OS X™ Mavericks 10.9	Die Trend Micro Security (für Mac)-Agents können jetzt auf Computern mit OS X™ Mavericks 10.9 installiert werden.

Trend Micro Security (für Mac) Server

Der Trend Micro Security (für Mac) Server ist der zentrale Speicherort für Informationen über alle vorhandenen Agent-Konfigurationen, Sicherheitsrisiko-Protokolle und Updates.

Der Server erfüllt zwei wichtige Funktionen:

- Überwacht und verwaltet Trend Micro Security (für Mac) Agents
- Lädt von Agents benötigte Komponenten herunter. Standardmäßig lädt der Trend Micro Security (für Mac) Server die Komponenten vom Trend Micro ActiveUpdate Server herunter und stellt sie dann den Agents zur Verfügung.

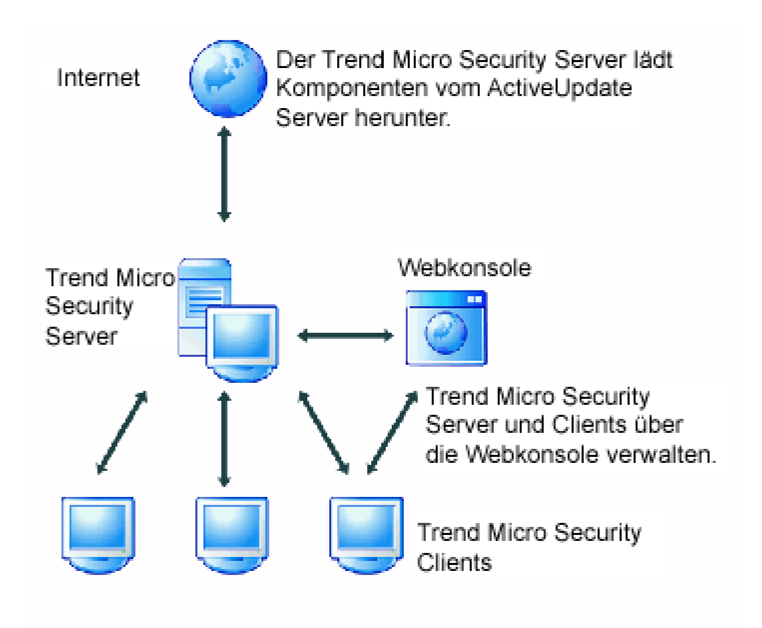


ABBILDUNG 1-1. Funktionsweise von Trend Micro Security (für Mac) Server

Trend Micro Security (für Mac) ermöglicht die bidirektionale Kommunikation zwischen Server und Agents in Echtzeit. Die Verwaltung der Agents erfolgt über eine browserbasierte Webkonsole, die Sie praktisch überall im Netzwerk aufrufen können. Server und Agent kommunizieren über das Protokoll ActiveMQ™.

Trend Micro Security (für Mac) Agent

Schützen Sie Ihre Mac-Computer vor Sicherheitsrisiken, indem Sie den Trend Micro Security (für Mac) Agent auf jedem Computer installieren. Der Agent stellt drei Suchmethoden zur Verfügung:

- Echtzeitsuche
- Zeitgesteuerte Suche
- Manuelle Suche

Der Agent berichtet an den übergeordneten Trend Micro Security (für Mac) Server, von dem aus er installiert wurde. Der Agent sendet Ereignis- und Statusinformationen in Echtzeit an den Server. Agents kommunizieren mit dem Server über das Protokoll ActivMQ.

Begriff

Die folgende Tabelle enthält offizielle Begriffe, die in der gesamten Trend Micro Security (für Mac) Dokumentation verwendet werden:

BEGRIFF	BESCHREIBUNG
Agent	Trend Micro Security (für Mac) Agent-Programm, das auf einem Mac-Computer installiert ist
Endpunkt	Mac-Computer, auf dem der Agent installiert ist
Agent-Benutzer (oder Benutzer)	Person, die den Agent auf dem Mac-Computer verwaltet
Server	Trend Micro Security (für Mac) Server-Programm
Server-Computer	Computer, auf dem der Trend Micro Security (für Mac) Server installiert ist
Administrator (oder Trend Micro Security (für Mac) Administrator)	Person, die den Trend Micro Security (für Mac) Server verwaltet
Konsole	Benutzerschnittstelle zur Konfiguration und Verwaltung der Trend Micro Security (für Mac) Server- und Agent-Einstellungen Die Konsole für das Serverprogramm wird ‚Webkonsole‘ genannt, die Konsole für den Agent heißt ‚Agent-Konsole‘.
Sicherheitsrisiko	Oberbegriff für Viren, Malware, Spyware/Grayware und Internet-Bedrohungen

Begriff	Beschreibung
Produktdienst	Trend Micro Security (für Mac) Dienst, der von der Microsoft Management Console (MMC) aus verwaltet wird
Komponenten	Suchen und entdecken Sicherheitsrisiken und führen Aktionen gegen sie durch.
`Agent-Installationsordner`	Ordner auf dem Mac-Computer, der die Programmdateien des Trend Micro Security (für Mac) Agents enthält `/Library/Application Support/TrendMicro`
`Server-Installationsordner`	Ordner auf dem Server-Computer, der die Programmdateien des Trend Micro Security (für Mac) Servers enthält Nach der Installation von Trend Micro Security (für Mac) Server wird der Ordner im gleichen Verzeichnis wie der Worry-Free Business Security Server-Ordner erstellt. Wenn Sie die Standardeinstellungen bei der Installation von Worry-Free Business Security übernehmen, ist der Server-Installationsordner einer der Folgenden: • `C:\Programme\Trend Micro\Security Server \Addon\TMSM` • `C:\Programme (x86)\Trend Micro\Security Server\Addon\TMSM`
Dualstapel	Entität, die sowohl IPv4- als auch IPv6-Adressen hat. Zum Beispiel: • Ein Dualstapel-Endpunkt ist ein Mac-Computer mit IPv4- und IPv6-Adressen. • Ein Dualstapel-Agent ist ein Agent, der auf einem Dualstapel-Endpunkt installiert ist. • Ein Dualstapel-Proxy-Server wie beispielsweise DeleGate kann IPv4- in IPv6-Adressen konvertieren und umgekehrt.
Reine IPv4	Entität, die nur eine IPv4-Adresse hat

BEGRIFF	BESCHREIBUNG
Reine IPv6	Entität, die nur eine IPv6-Adresse hat



Kapitel 2

Server installieren

In diesem Kapitel werden die Systemvoraussetzungen und die Installationsschritte für Trend Micro Security (für Mac) Server beschrieben.

Server-Installationsvoraussetzungen

Nachfolgend sind die Systemvoraussetzungen für die Installation von Trend Micro Security (für Mac) Server aufgeführt:

TABELLE 2-1. Server-Installationsvoraussetzungen

RESSOURCE	VORAUSSETZUNGEN
Worry-Free Business Security Server	9.0
Plug-in Manager	1.5
RAM	Mindestens 1 GB, 2 GB empfohlen
Verfügbarer Speicherplatz	• Mind. 1,5 GB, wenn der Worry-Free Business Security Server auf dem Systemlaufwerk installiert wird (in der Regel Laufwerk C:) • Wenn der Worry-Free Business Security Server nicht auf dem Systemlaufwerk installiert wird: • Mind. 600 MB auf dem Laufwerk, auf dem der Worry-Free Business Security Server installiert wird. Der Trend Micro Security (für Mac) Server wird auf diesem Laufwerk installiert. • Mindestens 900 MB auf dem Systemlaufwerk. Vom Trend Micro Security (für Mac) Server genutzte Programme von Drittanbietern werden auf diesem Laufwerk installiert.

Ressource	Voraussetzungen
Andere	• Microsoft™ .NET Framework 2.0 SP2 oder 3.5 SP1 • Microsoft Windows™ Installer 3.1 und höher • Java Runtime Environment™ (JRE) 1.6 oder höher mit dem aktuellsten Update **Hinweis** Installieren Sie JRE 1.7 oder höher, um eine möglichst hohe Leistung zu erzielen. Installieren Sie je nach dem Betriebssystem des Hostcomputers JRE für Windows x86 oder JRE für Windows x64. • Die folgenden Programme anderer Hersteller werden automatisch installiert, wenn sie nicht vorhanden sind: • Microsoft SQL Server 2005 oder 2008 R2 • Apache™ ActiveMQ 5.6.0 • Microsoft Visual C++ 2005 Redistributable

Update-Adresse

Plug-in Manager lädt das Installationspaket für Trend Micro Security (für Mac) von der Standard-WFBS-Update-Adresse herunter, wobei es sich um den Trend Micro ActiveUpdate Server handelt. Zur Änderung der Update-Adresse ändern Sie die folgende Einstellung in der Datei `<Installationsordner des WFBS Servers>\PCCSRV\Private\ofcserver.ini`:

```
[INI_UPDATE_SETTING]
PLMUpdateSource={Update-Server}
```

Ändern Sie beispielsweise `{Update-Server}` in:

`http://wfbs.activeupdate.example.com/activeupdate/wfbs`

Trend Micro Security (für Mac) Server installieren

Prozedur

1. Installation von Trend Micro Security (für Mac) auf einem Worry-Free Business Security Server:



Hinweis

Führen Sie die folgenden Schritte NUR aus, wenn Sie Trend Micro Security (für Mac) auf einem Server mit einer Domänencontroller-Rolle installieren.

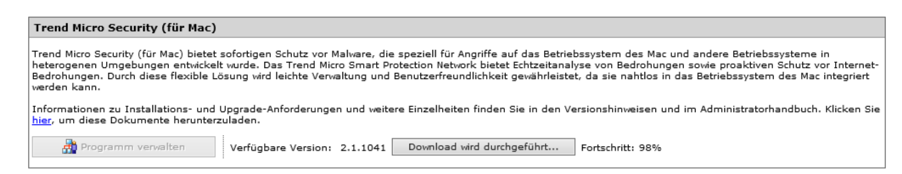
   a. Laden Sie die Datei InstallCfgFile.zip herunter.

   b. Entpacken Sie die `.ini`-Datei in den Ordner `...\Trend Micro \Security Server\PCCSRV\Admin\Utility\SQL\`.

2. Öffnen Sie die Worry-Free Business Security Webkonsole und klicken Sie im Hauptmenü auf **Voreinstellungen** > **Plug-ins**.



3. Klicken Sie im Abschnitt **Trend Micro Security (für Mac)** auf **Download**.



Die Größe der herunterzuladenden Datei wird neben der Schaltfläche **Download** angezeigt.

Der Plug-in Manager lädt das Paket in den Ordner <Installationsordner des WFBS Servers>\PCCSRV\Download\Product herunter.

Der <Installationsordner des WFBS Servers> ist normalerweise C:\Programme\Trend Micro\Security Server.

4. Verfolgen Sie den Download-Fortschritt.

   Trend Micro Security (für Mac) Download

   Trend Micro Security (für Mac) Version 2.1.1041 wird heruntergeladen. Bitte warten... Während des Downloads können Sie zu anderen Seiten navigieren.

   Fortschritt: 3%

   < Zurück

   Sie können während des Downloads zu anderen Fenstern navigieren.

   Wenn beim Herunterladen des Pakets Probleme auftreten, überprüfen Sie über die Worry-Free Business Security Webkonsole die Server-Update-Protokolle. Klicken Sie im Hauptmenü auf **Berichte** > **Protokollabfrage**.

5. Um Trend Micro Security (für Mac) sofort zu installieren, klicken Sie auf **Jetzt installieren** oder führen Sie folgende Vorgänge durch, um die Installation zu einem späteren Zeitpunkt durchzuführen:

   a. Klicken Sie auf **Später installieren**.

   b. Öffnen Sie das Fenster Plug-in Manager.

   c. Klicken Sie im Abschnitt **Trend Micro Security (für Mac)** auf **Installieren**.

6. Lesen Sie die Lizenzvereinbarung durch und nehmen Sie die Bedingungen durch Klicken auf **Stimme zu** an.



Die Installation beginnt.

7. Verfolgen Sie den Installationsfortschritt. Nach der Installation wird das Fenster Plug-in Manager neu geladen.

Tasks nach der Installation auf dem Server ausführen

Prozedur

1. Prüfen Sie, dass die folgenden Dienste auf der Microsoft Management Console angezeigt werden:

   - **ActiveMQ für Trend Micro Security**
   - **SQL Server (TMSM)**

- **Trend Micro Security für (Mac)**

2. Prüfen Sie im Windows Task Manager, dass der folgende Prozess ausgeführt wird: **TMSMMainService.exe**

3. Prüfen Sie im Registrierungs-Editor, dass der folgende Registrierungsschlüssel vorhanden ist: `HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_TMSM`

4. Prüfen Sie, dass die Dateien für Trend Micro Security (für Mac) Server im <*Server-Installationsordner*> vorhanden sind.

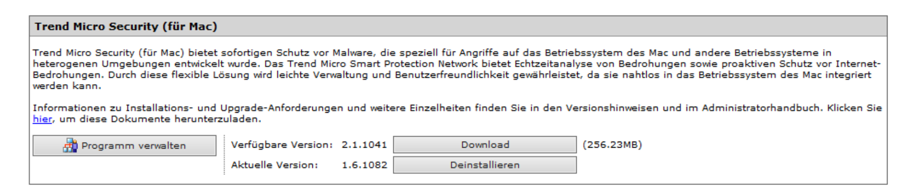
Trend Micro Security (für Mac) Server deinstallieren

Prozedur

1. Öffnen Sie die Worry-Free Business Security Webkonsole und klicken Sie im Hauptmenü auf **Voreinstellungen** > **Plug-Ins**.



2. Klicken Sie im Abschnitt **Trend Micro Security (für Mac)** auf **Deinstallieren**.



3. Verfolgen Sie den Deinstallationsfortschritt. Sie können während der Deinstallation zu anderen Fenstern navigieren. Nach Abschluss der Deinstallation kann der Trend Micro Security (für Mac) Server wieder installiert werden.



Hinweis

Die von Trend Micro Security (für Mac) genutzte Java Runtime Environment (JRE) wird vom Deinstallationspaket nicht entfernt. Falls sie von keiner anderen Anwendung benötigt wird, können Sie die JRE manuell entfernen.



Kapitel 3

Erste Schritte

In diesem Kapitel werden die ersten Schritte mit Trend Micro Security (für Mac) und Einstellungen für die Erstkonfiguration beschrieben.

Die Webkonsole

Die Webkonsole ist die zentrale Stelle zur Überwachung von Trend Micro Security (für Mac) Agents und zur Konfiguration der Einstellungen, die von den Agents übernommen werden. Sie enthält verschiedene Standardeinstellungen und -werte, die Sie entsprechend Ihren Sicherheitsanforderungen und -voraussetzungen konfigurieren können.

Über die Webkonsole können Sie folgende Aktionen ausführen:

- Auf Mac-Computern installierte Agents verwalten
- Agents zur gleichzeitigen Konfiguration und Verwaltung in logische Gruppen organisieren
- Auf einem oder mehreren Computern die Virensucheinstellungen festlegen und die Suche starten
- Benachrichtigungen über Sicherheitsrisiken konfigurieren und die von Agents gesendeten Protokolle anzeigen
- Ausbruchskriterien und -benachrichtigungen konfigurieren

Webkonsole öffnen

Vorbereitungen

Sie können die Webkonsole über jeden Computer im Netzwerk öffnen, der über die folgende Ausstattung verfügt:

- Monitor mit einer Mindestauflösung von 800 × 600 bei 256 Farben oder mehr
- Microsoft™ Internet Explorer™ 7.0 oder höher. Verwenden Sie auch für x64-Computer die 32-Bit-Version von Internet Explorer.

Prozedur

1. Geben Sie in einem Webbrowser die URL für den Worry-Free Business Security Server ein

2. Geben Sie den Benutzernamen und das Kennwort für die Anmeldung am Worry-Free Business Security Server ein.

3. Klicken Sie im Hauptmenü auf **Voreinstellungen** > **Plug-ins**.

4. Navigieren Sie zum Bereich **Trend Micro Security (für Mac)** und klicken Sie auf **Programm verwalten**.

Sicherheitszusammenfassung

Das Übersichtsfenster wird angezeigt, wenn Sie die Webkonsole von Trend Micro Security (für Mac) öffnen oder im Hauptmenü auf **Übersicht** klicken.



Tipp

Aktualisieren Sie dieses Fenster regelmäßig, um die aktuellsten Informationen zu erhalten.

Agents

Im Bereich **Agents** werden folgende Informationen angezeigt:

- Status der Verbindung zwischen allen Agents und dem Trend Micro Security (für Mac) Server: Durch Klicken auf einen Link wird die Agent-Struktur geöffnet, über die Sie Einstellungen für die Agents konfigurieren können.
- Anzahl der entdeckten Sicherheitsrisiken und Internetbedrohungen
- Anzahl der Computer mit entdeckten Sicherheitsrisiken und Internetbedrohungen. Durch Klicken auf eine Anzahl wird die Agent-Struktur geöffnet und eine Liste der Computer angezeigt, auf denen Sicherheitsrisiken und Internetbedrohungen entdeckt wurden. In der Agent-Struktur können Sie folgende Tasks ausführen:
    - Wählen Sie einen oder mehrere Agents aus, klicken Sie auf **Protokolle** > **Sicherheitsrisiko-Protokolle** und geben Sie die Protokollkriterien an. Überprüfen Sie im daraufhin angezeigten Fenster die Spalte **Ergebnisse**, um zu erkennen, ob die Suchaktionen bei den Sicherheitsrisiken erfolgreich durchgeführt wurden. Eine Liste aller Suchergebnisse finden Sie unter *Suchergebnis auf Seite 6-30*.

- Wählen Sie einen oder mehrere Agents aus, klicken Sie auf **Protokolle** > **Web-Reputation-Protokolle** und geben Sie die Protokollkriterien an. Prüfen Sie im daraufhin angezeigten Fenster die Liste der gesperrten Websites. Websites, die nicht gesperrt werden sollen, können der Liste der zulässigen URLs hinzugefügt werden. Weitere Informationen finden Sie unter *Liste der zulässigen URLs konfigurieren auf Seite 7-5*.

Update-Status

In der Tabelle **Update-Status** sind Informationen über die Komponenten von Trend Micro Security (für Mac) und das Agent-Programm enthalten, das Macintosh-Computer vor Sicherheitsrisiken schützt.

Tasks in dieser Tabelle:

- Aktualisieren Sie nicht aktuelle Komponenten sofort. Weitere Informationen finden Sie unter *Agent-Updates aus dem Übersichtsfenster starten auf Seite 5-12*.
- Aktualisieren Sie die Agent-Upgrades auf die aktuellste Programmversion bzw. den aktuellsten Build, wenn Sie kürzlich den Server aktualisiert haben. Eine Anleitung für Agent-Upgrades finden Sie unter *Server und Agents aktualisieren auf Seite 8-2*.

Agent-Struktur

Die Trend Micro Security (für Mac) Agent-Struktur zeigt alle Agents an, die der Server derzeit verwaltet. Alle Agents gehören einer bestimmten Gruppe an. Verwenden Sie die Menüeinträge über der Agent-Struktur, um eine Konfiguration gleichzeitig für alle Agents einer Gruppe zu konfigurieren, zu verwalten und anzuwenden.

Agent-Struktur – Allgemeine Tasks

Die folgende Übersicht enthält die allgemeinen Tasks, die Sie in der Agent-Struktur durchführen können:

Prozedur

- Klicken Sie auf das Stammsymbol ( ), um alle Gruppen und Agents auszuwählen. Wenn Sie zuerst das Stammsymbol und anschließend einen Menüeintrag über der

Agent-Struktur auswählen, wird ein Fenster mit den Konfigurationseinstellungen angezeigt. In diesem Fenster können Sie eine der folgenden allgemeinen Optionen auswählen:

- **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf neu zu einer vorhandenen/zukünftigen Gruppe hinzukommende Agents an. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
- **Nur auf zukünftige Gruppen anwenden**: Wendet Einstellungen nur auf Agents an, die zu zukünftigen Gruppen hinzugefügt wurden. Bei dieser Option werden die Einstellungen nicht auf neue Agents angewendet, die zu einer vorhandenen Gruppe hinzukommen.

- Klicken Sie zur Auswahl mehrerer aufeinander folgender Gruppen oder Agents auf die erste Gruppe oder den ersten Agent des Bereichs. Halten Sie die Umschalttaste gedrückt und klicken Sie dann auf die letzte Gruppe oder den letzten Agent des Bereichs.
- Um mehrere nicht unmittelbar aufeinander folgende Gruppen oder Agents auszuwählen, halten Sie die Strg-Taste gedrückt und klicken auf die gewünschten Gruppen oder Agents.
- Sie können nach einem bestimmten zu verwaltenden Agent suchen, indem Sie seinen vollständigen Namen oder einen Teil des Namens in das Textfeld **Nach Computern suchen** eingeben. In der Agent-Struktur wird eine Liste mit übereinstimmenden Agent-Namen angezeigt.



Hinweis

IPv6- oder IPv4-Adressen können nicht angegeben werden, wenn nach bestimmten Agents gesucht wird.

- Sie können Agents durch Klicken auf den Spaltennamen nach den Informationen in den Spalten sortieren.
- Zeigen Sie die Gesamtanzahl der Agents unter der Agent-Struktur an.

Agent-Struktur – Besondere Tasks

Über der Agent-Struktur befinden sich Menüeinträge, mit denen Sie folgende Tasks durchführen können:

MENÜSCHALTFLÄCHE	TASK
Tasks	• Agent-Komponenten aktualisieren. Weitere Informationen finden Sie unter *Agent-Updates auf Seite 5-8*. • ‚Jetzt durchsuchen' auf Mac-Computern durchführen. Weitere Informationen finden Sie unter *Jetzt durchsuchen auf Seite 6-9*.
Einstellungen	• Sucheinstellungen konfigurieren. • *Manuelle Suche auf Seite 6-7* • *Echtzeitsuche auf Seite 6-5* • *Zeitgesteuerte Suche auf Seite 6-8* • *Suchausschlüsse auf Seite 6-18* • *Zwischenspeicher-Einstellungen für Suchen auf Seite 6-23* • Web-Reputation-Einstellungen konfigurieren. Weitere Informationen finden Sie unter *Einstellungen für Web Reputation konfigurieren auf Seite 7-3*. • Aktualisierungseinstellungen konfigurieren. Weitere Informationen finden Sie unter *Agent-Update-Einstellungen konfigurieren auf Seite 5-10*.
Protokolle	Sehen Sie die Protokolle ein. • *Sicherheitsrisiko-Protokolle anzeigen auf Seite 6-29* • *Web-Reputation-Protokolle anzeigen auf Seite 7-6*
Agent-Struktur verwalten	Trend Micro Security (für Mac) Gruppen verwalten. Weitere Informationen finden Sie unter *Gruppen auf Seite 3-7*.

Gruppen

Eine Gruppe in Trend Micro Security (für Mac) umfasst eine Gruppe von Agents mit derselben Konfiguration, die die gleichen Tasks ausführen. Durch die Übersicht der Agents in Gruppen kann die Konfiguration für alle Agents einer Gruppe gleichzeitig konfiguriert, verwaltet und angewandt werden.

Agents können einfacher verwaltet werden, wenn Sie diese nach Abteilungszugehörigkeit oder Aufgabenbereich gruppieren. So können stärker gefährdete Agents in einer Gruppe zusammengefasst werden, damit Sie für alle einen höheren Schutz konfigurieren können. Sie können Gruppen hinzufügen und umbenennen sowie Agents in andere Gruppen verschieben oder auch dauerhaft entfernen. Ein aus der Agent-Struktur entfernter Agent wird nicht automatisch vom Mac-Computer deinstalliert. Der Agent kann noch immer serverabhängige Funktionen durchführen, wie das Update der Komponenten. Der Server weiß jedoch nicht, dass der Agent vorhanden ist, und kann ihm daher keine Konfigurationen oder Benachrichtigungen senden.

Wenn ein Agent vom Mac-Computer deinstalliert wurde, wird er nicht automatisch aus der Agent-Struktur entfernt, und sein Verbindungsstatus wird in „Offline" geändert. Sie müssen den Agent manuell aus der Agent-Struktur entfernen.

Gruppen hinzufügen

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie auf **Agent-Struktur verwalten** > **Gruppe hinzufügen**.
3. Geben Sie einen Namen für die Gruppe ein, die Sie hinzufügen möchten.
4. Klicken Sie auf **Hinzufügen**.

   Die neue Gruppe wird nun in der Agent-Struktur angezeigt.

Gruppen oder Agents löschen

Vorbereitungen

Vergewissern Sie sich vor dem Löschen einer Gruppe, ob in dieser noch Agents enthalten sind, und verschieben Sie diese wenn nötig in eine andere Gruppe. Details zum Verschieben von Agents finden Sie unter *Agents verschieben auf Seite 3-9*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Wählen Sie in der Agent-Struktur bestimmte Gruppen oder Agents auf.
3. Klicken Sie auf **Agent-Struktur verwalten** > **Gruppe/Agent entfernen**.
4. Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Gruppen umbenennen

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Wählen Sie in der Agent-Struktur die Gruppe aus, die Sie umbenennen möchten.
3. Klicken Sie auf **Agent-Struktur verwalten** > **Gruppe umbenennen**.
4. Geben Sie einen neuen Namen für die Gruppe ein.
5. Klicken Sie auf **Umbenennen**.

   Der neue Gruppenname wird nun in der Agent-Struktur angezeigt.

Agents verschieben

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Wählen Sie in der Agent-Struktur einen oder mehrere Agents aus, die zu einer Gruppe gehören.
3. Klicken Sie auf **Agent-Struktur verwalten** > **Agent verschieben**.
4. Wählen Sie die Gruppe aus, in die Sie den Agent verschieben möchten.
5. Legen Sie fest, ob die Einstellungen der neuen Gruppe auf den Agent angewendet werden sollen.



Tipp

Tipp: Sie können Agents auch per Drag & Drop in eine andere Gruppe innerhalb der Agent-Struktur verschieben.

6. Klicken Sie auf **Verschieben**.

Trend Micro Smart Protection

Trend Micro Smart Protection ist eine cloudbasierte Content-Security-Infrastruktur der neuesten Generation zum Schutz vor Sicherheitsrisiken und Bedrohungen aus dem Internet. Sie umfasst sowohl lokale als auch gehostete Lösungen und bietet umfassenden Schutz im Netzwerk, zu Hause oder unterwegs. Über schlanke Clients erhalten die Benutzer Zugriff zu einer einzigartigen Kombination aus E-Mail-, Web- und File-Reputationstechnologien sowie Bedrohungsdatenbanken in der Cloud. Je mehr Produkte, Dienste und Benutzer auf das Netzwerk zugreifen, desto weiter werden die stets automatisch aktualisierten Schutzfunktionen ausgebaut. So entsteht eine Art digitale „Nachbarschaftswache“ in Echtzeit.

Smart Protection-Dienste

Zu den Smart Protection-Diensten zählen File-Reputation-Dienste, Web-Reputation-Dienste und Smart Feedback.

In dieser Version stellen Trend Micro Security (für Mac) Agents mit Hilfe der *Web-Reputation-Dienste auf Seite 7-2* fest, ob Websites, auf die über einen Mac-Computer zugegriffen wird, auch wirklich sicher sind.

Smart Protection-Quellen

Die Bereitstellung der Web-Reputation-Dienste erfolgt durch **Trend Micro Smart Protection Network**.

Trend Micro Smart Protection Network ist eine global skalierte, internetbasierte Infrastruktur, die sich an Benutzer ohne direkten Zugang zu ihrem Unternehmensnetzwerk richtet.

Smart Protection-Quelle für externe oder interne Agents

Externe Agents (d. h. Agents ohne funktionsfähige Verbindung mit dem Trend Micro Security (für Mac) Server) oder interne Agents (d. h. Agents mit funktionsfähiger Verbindung mit dem Trend Micro Security (für Mac) Server) senden Web-Reputation-Abfragen an das Smart Protection Network. Zum Versand von Abfragen ist allerdings eine Internetverbindung erforderlich.

Aktivieren Sie im Fenster der Web-Reputation-Dienste die Web-Reputation-Richtlinie für externe Agents. Detaillierte Anweisungen dazu finden Sie unter *Einstellungen für Web Reputation konfigurieren auf Seite 7-3*.



Kapitel 4

Agent installieren

Dieses Kapitel beschreibt Anforderungen und Vorgehensweisen für die Installation von Trend Micro Security (für Mac) Agent.

Informationen zum Aktualisieren des Agents finden Sie unter *Server und Agents aktualisieren auf Seite 8-2*.

Voraussetzungen für die Installation des Agents

Nachfolgend sind die Systemvoraussetzungen für die Installation des Trend Micro Security (für Mac) Agents auf einem Mac-Computer aufgeführt.

TABELLE 4-1. Voraussetzungen für die Installation des Agents

RESSOURCE	VORAUSSETZUNG
Betriebssystem	• OS X™ Mavericks 10.9 oder höher • OS X™ Mountain Lion 10.8.3 oder höher • Mac OS X™ Lion 10.7.5 oder höher • Mac OS X Snow Leopard™ 10.6.8 oder höher • Mac OS X Leopard™ 10.5.8 oder höher
Hardware	• **Prozessor**: Intel™ Core-Prozessor • **RAM**: Mindestens 256 MB • **Verfügbarer Speicherplatz**: Mindestens 30 MB



Hinweis

Diese Produktversion unterstützt Mac OS X Tiger™ 10.4.11 und PowerPC™-Prozessor nicht mehr. Falls Agents auf Mac OS X Tiger installiert sind und/oder ein PowerPC-Prozessor verwendet wird, aktualisieren Sie die Agents nicht und stellen Sie sicher, dass ein Trend Micro Security (für Mac) 1.x Server zur Verwaltung dieser Agents vorhanden ist.

Methoden und Setup-Dateien zur Agent-Installation

Es gibt zwei Möglichkeiten zur Installation des Trend Micro Security (für Mac) Agents.

- Installation auf einem einzelnen Computer durch Starten des Installationspakets (`tmsminstall.zip`) auf dem Mac-Computer

- Installation auf verschiedenen Computern durch Starten des Installationspakets (`tmsminstall.mpkg.zip`) über Apple Remote Desktop



Hinweis

Informationen zum Upgrade von Agents finden Sie unter *Server und Agents aktualisieren auf Seite 8-2*.

Laden Sie das nötige Agent-Installationspaket vom Trend Micro Security (für Mac) Server herunter und kopieren Sie es auf den Mac-Computer.

Es gibt zwei Möglichkeiten, das Paket zu beziehen:

- Öffnen Sie die Trend Micro Security (für Mac) Webkonsole, gehen Sie zu **Administration** > **Agent-Installationsdateien** und klicken Sie unter **Agent-Installationsdatei** auf einen Link.

  Hinweis

  Die Links zu den Agent-Deinstallationspaketen werden ebenfalls in diesem Fenster angezeigt. Verwenden Sie diese Pakete zum Entfernen des Agent-Programms von den Mac-Computern. Wählen Sie das Paket je nach Version des Agent-Programms, das Sie entfernen möchten. Informationen zur Deinstallation des Trend Micro Security (für Mac) Agents finden Sie unter *Agent-Deinstallation auf Seite 4-14*.

- Wechseln Sie zu <*Server-Installationsordner*>`\TMSM_HTML\ClientInstall`.

Auf einem einzelnen Mac-Computer installieren

Die Installation des Trend Micro Security (für Mac) Agents auf einem einzelnen Computer ist vergleichbar mit der Installation anderer Mac-Software.

Während der Installation wird der Benutzer möglicherweise aufgefordert, Verbindungen zu **iCoreService** zu erlauben. Diese Komponente wird zur Registrierung des Agents am Server verwendet. Weisen Sie die Benutzer an, diese Verbindung zuzulassen.

Prozedur

1. Suchen Sie zunächst sämtliche, bereits auf dem Mac-Computer installierte Sicherheitssoftware und deinstallieren Sie diese.

2. Laden Sie das Agent-Installationspaket `tmsminstall.zip` herunter.

   Weitere Informationen zum Erhalt des Pakets finden Sie unter *Methoden und Setup-Dateien zur Agent-Installation auf Seite 4-2*.

3. Kopieren Sie `tmsminstall.zip` auf den Mac-Computer und starten Sie es dann über das integrierte Archivierungsprogramm.



Warnung!

Die Dateien im Paket `tmsminstall.zip` können beschädigt werden, wenn das Paket nicht mit einem integrierten Mac-Archivierungsprogramm geöffnet wird.

Um das Paket `tmsminstall.zip` in einem Terminalfenster zu starten, verwenden Sie folgenden Befehl:

```
ditto -xk <tmsminstall.zip file path> <destination folder>
```

Zum Beispiel:

```
ditto -xk users/mac/Desktop/tmsminstall.zip users/mac/Desktop
```

Durch den Start von `tmsminstall.zip` wird ein neuer Ordner `tmsminstall` erstellt.

4. Öffnen Sie den Ordner `tmsminstall` und starten Sie `tmsminstall.pkg`.

5. Wenn Sie gefragt werden, ob Sie mit der Installation fortfahren möchten, klicken Sie auf **Fortfahren**.



6. Klicken Sie im Einführungsfenster auf **Fortfahren**.



7. Lesen Sie die Erinnerungsnachrichten und klicken Sie auf **Weiter**.



8. Klicken Sie im Fenster Installationstyp auf **Installieren**.

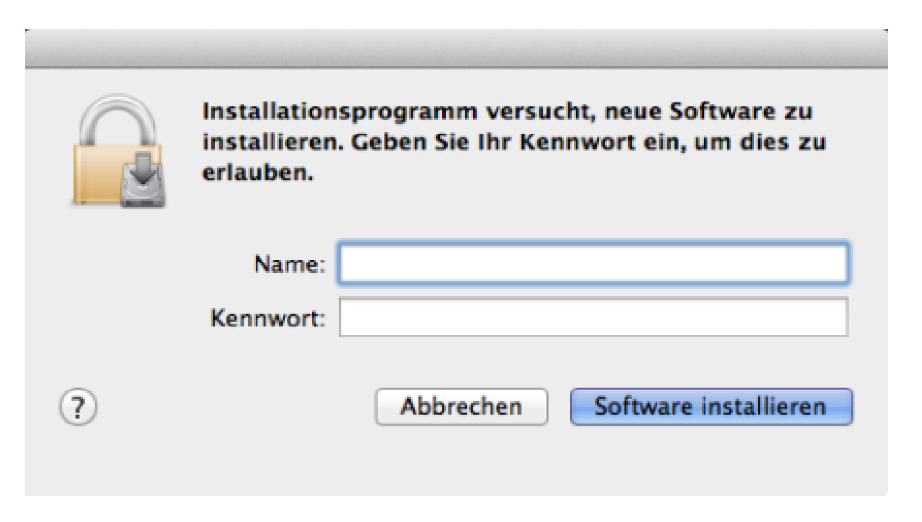


9. Tragen Sie den **Name** und das **Kennwort** in die entsprechenden Felder ein, um die Installation zu starten.

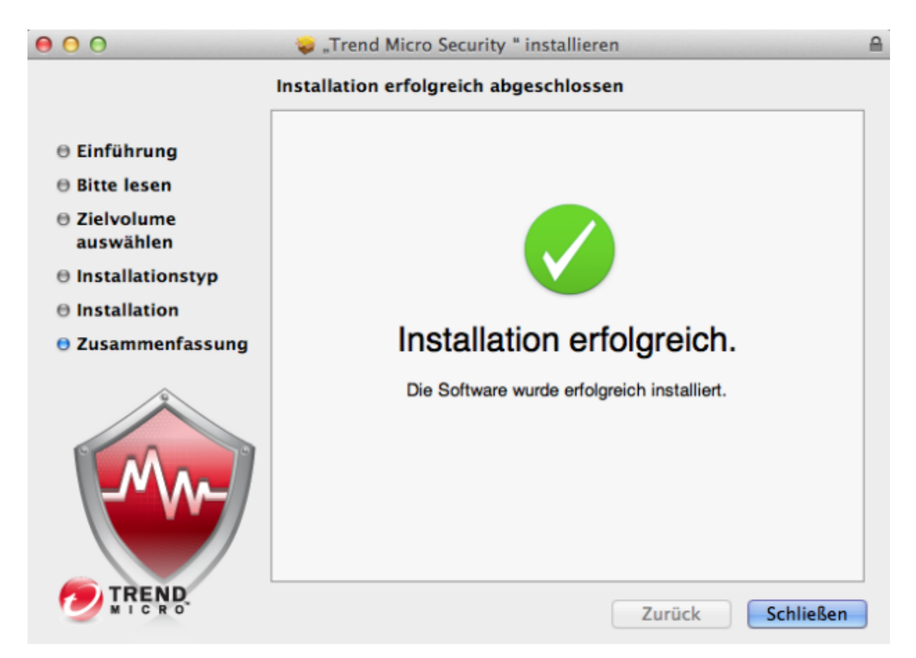


Hinweis

Geben Sie den Namen und das Kennwort für ein Konto mit Administratorrechten auf dem Mac-Computer an.



10. Klicken Sie nach erfolgreicher Installation auf **Schließen**, um die Installation abzuschließen.



Der Agent registriert sich automatisch an dem Server, von dem das Agent-Installationspaket heruntergeladen wurde. Außerdem aktualisiert sich der Agent zum ersten Mal.

Nächste Maßnahme

Führen Sie für den Agent Tasks nach der Installation durch. Weitere Informationen finden Sie unter *Vorgänge nach der Agent-Installation auf Seite 4-12*.

Auf mehreren Mac-Computern installieren

Die Installation des Trend Micro Security (für Mac) Agents auf mehreren Computern kann mit Hilfe von Apple Remote Desktop vereinfacht werden.



Hinweis

Falls Mac-Computer nur eine IPv6-Adresse besitzen, lesen Sie die IPv6-Einschränkungen für die Agent-Bereitstellung mit Apple Remote Desktop in *Einschränkungen eines reinen IPv6-Agents auf Seite A-3* durch.

Prozedur

1. Suchen Sie zunächst sämtliche, bereits auf dem Mac-Computer installierte Sicherheitssoftware und deinstallieren Sie diese.

2. Laden Sie das Agent-Installationspaket `tmsminstall.mpkg.zip` herunter. Informationen zum Herunterladen dieses Pakets finden Sie unter *Methoden und Setup-Dateien zur Agent-Installation auf Seite 4-2*.

3. Kopieren Sie `tmsminstall.mpkg.zip` mit Apple Remote Desktop auf den Mac-Computer und starten Sie es dann über das integrierte Archivierungsprogramm.



Warnung!

Die Dateien im Paket `tmsminstall.mpkg.zip` können beschädigt werden, wenn das Paket nicht mit einem integrierten Mac-Archivierungsprogramm geöffnet wird.

Um das Paket `tmsminstall.mpkg.zip` in einem Terminalfenster zu starten, verwenden Sie folgenden Befehl:

```
ditto -xk <tmsminstall.mpkg.zip file path> <destination
folder>
```

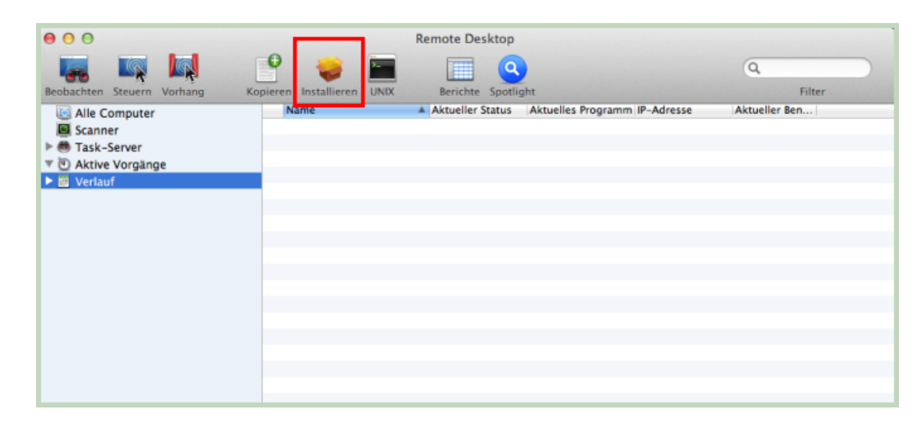
Zum Beispiel:

```
ditto -xk users/mac/Desktop/tmsminstall.mpkg.zip users/mac/
Desktop
```

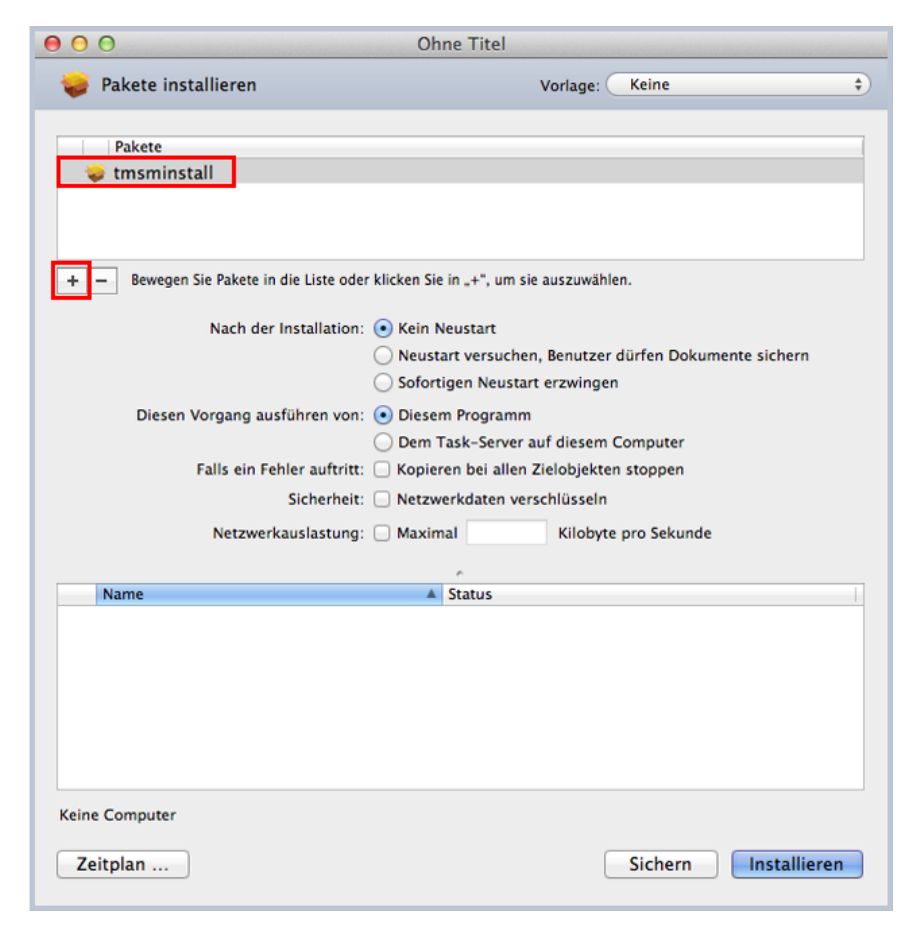
Durch Starten des Pakets `tmsminstall.mpkg.zip` wird die Datei `tmsminstall.mpkg` extrahiert.

4. Öffnen Sie Apple Remote Desktop auf dem Mac-Computer.

5. Wählen Sie die Computer aus, auf denen Sie den Trend Micro Security (für Mac) Agent installieren möchten, und klicken Sie auf **Installieren**.



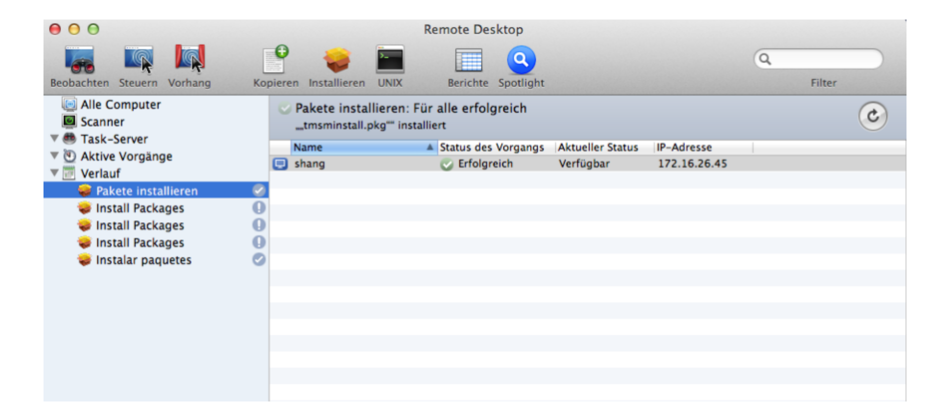
6. Ziehen Sie das Installationspaket ins Fenster Pakete installieren, oder klicken Sie auf ‚+', um das Installationspaket zu suchen.



7. (Optional) Klicken Sie auf **Sichern**, um die Installation automatisch auf allen neuen Mac-Computern durchzuführen, die mit dem Netzwerk verbunden sind.

8. Klicken Sie auf **Installieren**.

   Der Apple Remote Desktop beginnt mit der Installation des Agents auf den ausgewählten Computern. Nach erfolgreicher Installation auf allen Computern erscheint die Meldung `Install Packages: Succeeded on all`. Andernfalls erscheint die Meldung `Successful` im Abschnitt **Status des Vorgangs** jedes Computers, auf dem die Installation erfolgreich durchgeführt wurde.



Die Agents registrieren sich automatisch an dem Server, von dem das Agent-Installationspaket heruntergeladen wurde. Außerdem aktualisieren sich die Agents zum ersten Mal.

Nächste Maßnahme

Führen Sie für den Agent Tasks nach der Installation durch. Weitere Informationen finden Sie unter *Vorgänge nach der Agent-Installation auf Seite 4-12*.

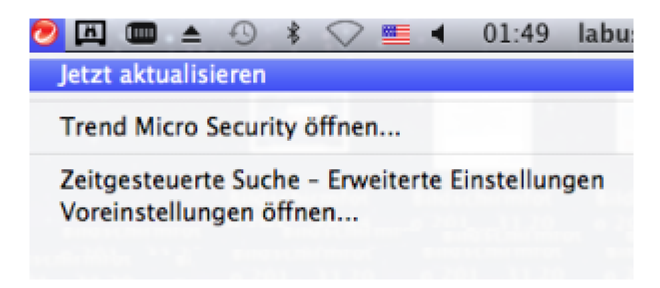
Vorgänge nach der Agent-Installation

Prozedur

1. Überprüfen Sie Folgendes:

- Das Symbol des Trend Micro Security (für Mac) Agents ( ) wird in der Menüleiste des Mac-Computers angezeigt.
- Die Dateien zum Trend Micro Security (für Mac) Agent befinden sich im <*Agent-Installationsordner*>.
- Der Agent wird in der Agent-Struktur der Webkonsole angezeigt. Klicken Sie im Hauptmenü auf **Agent-Verwaltung**, um die Agent-Struktur anzuzeigen.

2. Aktualisierung der Trend Micro Security (für Mac) Komponenten. Der Agent lädt Komponenten vom Trend Micro Security (für Mac) Server herunter. Weitere Informationen finden Sie unter *Agent-Updates auf Seite 5-8*.



Wenn der Agent keine Verbindung zum Server herstellen kann, lädt er die Dateien direkt vom Trend Micro ActiveUpdate Server herunter. Für die Verbindung zum ActiveUpdate Server ist eine Internetverbindung notwendig.

3. Starten Sie Jetzt durchsuchen auf dem Mac-Computer oder weisen Sie den Benutzer an, eine manuelle Suche durchzuführen.



Nächste Maßnahme

Wenn nach der Installation des Agents Probleme auftreten, deinstallieren Sie ihn und installieren Sie ihn erneut.

Agent-Deinstallation

Deinstallieren Sie den Agent nur, wenn Probleme mit dem Programm auftreten. Installieren Sie ihn anschließen umgehend erneut, damit Ihr Computer weiterhin vor Sicherheitsrisiken geschützt ist.

Prozedur

1. Laden Sie das Agent-Deinstallationspaket `tmsmuninstall.mpkg.zip` vom Trend Micro Security (für Mac) Server herunter. Öffnen Sie die Trend Micro Security (für Mac) Webkonsole, gehen Sie zu **Administration** > **Agent-Installationsdateien** und klicken Sie unter **Agent-Deinstallationsdatei** auf den Link.

2. Kopieren Sie das Paket auf den Mac-Computer und starten Sie es.

3. Tragen Sie den **Namen** und das **Kennwort** in die entsprechenden Felder ein, um die Deinstallation zu starten.

   Hinweis

   Geben Sie den Namen und das Kennwort für ein Konto mit Administratorrechten auf dem Mac-Computer an.

4. Klicken Sie nach erfolgreicher Deinstallation auf **Schließen**, um die Deinstallation abzuschließen.

Nächste Maßnahme

Melden Sie den Agent vom Server ab.

1. Klicken Sie in der Webkonsole auf **Agent-Verwaltung** und wählen Sie den deinstallierten Agent aus.

2. Klicken Sie auf **Agent-Struktur verwalten** > **Gruppe/Agent entfernen**.



Kapitel 5

Den Schutz auf dem neuesten Stand halten

In diesem Kapitel werden die Trend Micro Security (für Mac) Komponenten und Update-Verfahren erläutert.

Komponenten

Trend Micro Security (für Mac) besteht aus mehreren Komponenten, die zusammen Agents vor den aktuellen Sicherheitsrisiken schützen. Halten Sie diese Komponenten mit manuellen oder zeitgesteuerten Updates auf dem neuesten Stand.

Zusätzlich zu den Komponenten erhalten Trend Micro Security (für Mac) Agents aktualisierte Konfigurationsdateien vom Trend Micro Security (für Mac) Server. Agents benötigen diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der Trend Micro Security (für Mac) Einstellungen über die Webkonsole ändern sich auch die Konfigurationsdateien.

Viren-Pattern

Das Viren-Pattern enthält Informationen, mit denen Trend Micro Security (für Mac) die neuesten Viren- und Malware-Programme sowie kombinierte Angriffe erkennt. Mehrmals pro Woche und bei jeder Entdeckung besonders schädlicher Viren- oder Malware-Programme erstellt und veröffentlicht Trend Micro ein neues Viren-Pattern.

Spyware-Aktivmonitor-Pattern

Das Spyware-Aktivmonitor-Pattern enthält Informationen, mit denen Trend Micro Security (für Mac) Spyware und Grayware erkennt.

Viren-Scan-Engine

Die Viren-Scan-Engine bildet den Kern aller Trend Micro-Produkte. Sie wurde ursprünglich als Reaktion auf die ersten dateibasierten Computerviren entwickelt. Heute ist die Scan-Engine technisch so ausgefeilt, dass sie verschiedenste Sicherheitsrisiken einschließlich Spyware erkennt. Die Viren-Scan-Engine erkennt auch kontrollierte Viren, die zu Forschungszwecken entwickelt und verwendet werden.

Die Scan-Engine aktualisieren

Da die zeitkritischsten Informationen über Sicherheitsrisiken in den Pattern-Dateien gespeichert sind, kann Trend Micro die Anzahl der Scan-Engine-Updates auf ein Mindestmaß reduzieren und gleichzeitig ein hohes Schutzniveau beibehalten. Dennoch stellt Trend Micro in regelmäßigen Abständen neue Versionen der Scan-Engine zur Verfügung, und zwar in den folgenden Fällen:

- Neue Technologien zur Suche und Entdeckung von Viren werden in die Software integriert.
- Neue, potenziell gefährliche Sicherheitsrisiken wurden entdeckt, auf welche die Scan Engine nicht reagieren kann.
- Die Suchleistung wurde verbessert.
- Neue Dateiformate, Skriptsprachen, Kodierungen und/oder Komprimierungsformate werden hinzugefügt.

Agent-Programm

Das Trend Micro Security (für Mac) Agent-Programm bietet den eigentlichen Schutz vor Sicherheitsrisiken.

Update-Übersicht

Alle Komponenten-Updates stammen vom Trend Micro ActiveUpdate Server. Wenn Updates verfügbar sind, lädt der Trend Micro Security (für Mac) Server die aktualisierten Komponenten herunter.

Der Trend Micro Security (für Mac) Server kann so konfiguriert werden, dass Updates von einer anderen Adresse als dem Trend Micro ActiveUpdate Server bezogen werden. Dafür müssen Sie eine benutzerdefinierte Update-Adresse einrichten. Wenden Sie sich an Ihren Support-Anbieter, um Unterstützung beim Einrichten dieser Update-Adresse zu erhalten.

In der folgenden Tabelle werden verschiedene Optionen für Komponenten-Updates für die Trend Micro Security (für Mac) Server und Agents beschrieben:

TABELLE 5-1. Server-/Agent-Update-Optionen

UPDATE-OPTION	BESCHREIBUNG
ActiveUpdate Server ↓ Trend Micro Security (für Mac) Server ↓ Agents	Der Trend Micro Security (für Mac) Server empfängt aktualisierte Komponenten vom Trend Micro ActiveUpdate Server (oder einer anderen Update-Adresse, wenn eine solche eingerichtet wurde) und verteilt diese dann an die Agents.
ActiveUpdate Server ↓ Agents	Trend Micro Security (für Mac) Agents erhalten die aktualisierten Komponenten direkt vom ActiveUpdate Server, wenn sie keine Verbindung zum Trend Micro Security (für Mac) Server herstellen können.

Server-Update

Der Trend Micro Security (für Mac) Server lädt die folgenden Komponenten herunter und verteilt sie an die Agents:

- Viren-Pattern
- Spyware-Aktivmonitor-Pattern
- Viren-Scan-Engine

Sie können die aktuellen Versionen der Komponenten in der Webkonsole im Übersichtsfenster anzeigen und die Anzahl der Agents mit oder ohne aktuelle Komponenten bestimmen.

Wenn die Verbindung zum Internet über einen Proxy-Server hergestellt wird, müssen Sie für den Download der Updates die korrekten Proxy-Einstellungen verwenden.

Update-Adresse des Servers konfigurieren

Sie können den Trend Micro Security (für Mac) Server so konfigurieren, dass die Komponenten vom Trend Micro ActiveUpdate Server oder einer anderen Adresse heruntergeladen werden.



Hinweis

Wenn der Server ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Server-Updates in *Einschränkungen eines reinen IPv6-Servers auf Seite A-3*.

Nach dem Download verfügbarer Updates benachrichtigt der Server automatisch die Agents, damit diese die Updates ihrer Komponenten durchführen. Ist das Komponenten-Update kritisch, sollte der Server die Agents umgehend benachrichtigen. Die entsprechenden Einstellungen nehmen Sie unter **Agent-Verwaltung** > **Tasks** > **Update** vor.

Prozedur

1. Gehen Sie zu **Server-Updates** > **Update-Adresse**.
2. Wählen Sie den Ort aus, von dem das Update heruntergeladen werden soll.
    - Bei Auswahl von ActiveUpdate Server:
        - Stellen Sie sicher, dass der Trend Micro Security (für Mac) Server mit dem Internet verbunden ist.
        - Wenn Sie einen Proxy-Server verwenden, testen Sie die Internetverbindung mit den betreffenden Proxy-Einstellungen. Weitere Informationen finden Sie unter *Proxy-Einstellungen für Server-Updates konfigurieren auf Seite 5-6*.
    - Bei Auswahl einer benutzerdefinierten Update-Adresse:

- Richten Sie die betreffende Umgebung und die erforderlichen Update-Ressourcen ein.
- Stellen Sie sicher, dass der Servercomputer mit dieser Update-Adresse verbunden ist. Wenden Sie sich an Ihren Support-Anbieter, um Unterstützung beim Einrichten einer Update-Adresse zu erhalten.

3. Klicken Sie auf **Speichern**.

Proxy-Einstellungen für Server-Updates konfigurieren

Sie können den Trend Micro Security (für Mac) Server so konfigurieren, dass für den Download der Updates vom Trend Micro ActiveUpdate Server die Proxy-Einstellungen verwendet werden.



Hinweis

Wenn der Server ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Proxy-Einstellungen in *Einschränkungen eines reinen IPv6-Servers auf Seite A-3*.

Prozedur

1. Gehen Sie zu **Administration** > **Externe Proxy-Einstellungen**.
2. Aktivieren Sie das Kontrollkästchen für die Verwendung eines Proxy-Servers.
3. Geben Sie den Namen oder die IPv4- bzw. IPv6-Adresse des Proxy-Servers und seine Portnummer an.
4. Falls der Proxy-Server einen Benutzernamen und ein Kennwort erfordert, geben Sie diese in die dafür vorgesehenen Textfelder ein.
5. Klicken Sie auf **Speichern**.

Server-Update-Methoden

Sie können das Update der Komponenten von Trend Micro Security (für Mac) Server manuell oder zeitgesteuert durchführen.

- **Manuelles Update**: Führen Sie ein manuelles Update durch, wenn ein Update kritisch ist, damit der Server die Updates umgehend beziehen kann. Weitere Informationen finden Sie unter *Server manuell aktualisieren auf Seite 5-8*.
- **Zeitgesteuertes Update**: Der Trend Micro Security (für Mac) Server stellt am geplanten Tag und zur geplanten Uhrzeit eine Verbindung zur Update-Adresse her, um die aktuellsten Komponenten herunterzuladen. Weitere Informationen finden Sie unter *Server-Updates zeitlich planen auf Seite 5-7*.

Nachdem ein Server-Update abgeschlossen ist, wird der Agent umgehend zum Update aufgefordert.

Server-Updates zeitlich planen

Sie können den Trend Micro Security (für Mac) Server so konfigurieren, dass er seine Update-Adresse regelmäßig überprüft und verfügbare Updates automatisch herunterlädt. Durch das zeitgesteuerte Server-Update können Sie einfach und wirksam sicherstellen, dass Ihr Schutz vor Sicherheitsrisiken immer auf dem neuesten Stand ist.

Nachdem ein Server-Update abgeschlossen ist, wird der Agent zum Update aufgefordert.

Prozedur

1. Gehen Sie zu **Server-Updates** > **Zeitgesteuertes Update**.
2. Wählen Sie die zu aktualisierenden Komponenten aus.
3. Geben Sie den Update-Zeitplan an.

   Bei täglichen, wöchentlichen und monatlichen Updates gibt der Zeitraum die Anzahl der Stunden an, in denen Trend Micro Security (für Mac) das Update durchführt. Trend Micro Security (für Mac) führt das Update zu einem beliebigen Zeitpunkt innerhalb dieses Zeitraums durch.

Wenn Sie für die monatlichen Updates den 29., 30. oder 31. Tag des Monats ausgewählt haben, dieser Tag im betreffenden Monat jedoch nicht vorkommt, führt Trend Micro Security (für Mac) das Update am letzten Tag des Monats durch.

4. Klicken Sie auf **Speichern**.

Server manuell aktualisieren

Führen Sie nach der Installation oder einem Upgrade von Trend Micro Security (für Mac) Server sowie bei einem Ausbruch ein manuelles Update der Komponenten auf dem Server durch.

Prozedur

1. Gehen Sie zu **Server-Updates** > **Manuelles Update**.
2. Wählen Sie die zu aktualisierenden Komponenten aus.
3. Klicken Sie auf **Update**.

   Der Server lädt die aktualisierten Komponenten herunter.

   Nachdem ein Server-Update abgeschlossen ist, wird der Agent umgehend zum Update aufgefordert.

Agent-Updates

Um sicherzustellen, dass Agents vor den neuesten Sicherheitsrisiken geschützt sind, müssen Sie die Agent-Komponenten regelmäßig aktualisieren. Aktualisieren Sie die Agents auch, wenn die Komponenten stark veraltet sind oder ein Ausbruch auftritt. Komponenten veralten stark, wenn der Agent seine Komponenten über einen längeren Zeitraum nicht über den Trend Micro Security (für Mac) Server oder den ActiveUpdate Server aktualisieren kann.

Agent-Update-Methoden

Es gibt mehrere Möglichkeiten, Agent-Updates durchzuführen.

UPDATE-METHODE	BESCHREIBUNG
Vom Administrator eingeleitetes manuelles Update	Updates können in den folgenden Webkonsolen-Fenstern gestartet werden: • Agent-Verwaltung: Weitere Informationen finden Sie unter *Agent-Updates aus dem Agent-Verwaltung-Fenster starten auf Seite 5-12*. • Übersicht: Weitere Informationen finden Sie unter *Agent-Updates aus dem Übersichtsfenster starten auf Seite 5-12*.
Automatisches Update	• Nachdem ein Server-Update abgeschlossen ist, wird der Agent umgehend zum Update aufgefordert. • Die Updates können anhand eines von Ihnen konfigurierten Zeitplans durchgeführt werden. Der konfigurierte Zeitplan kann auf eine(n) oder auf mehrere Agents oder Domänen oder auf alle vom Server verwalteten Agents angewendet werden. Weitere Informationen finden Sie unter *Agent-Update-Einstellungen konfigurieren auf Seite 5-10*.
Vom Benutzer eingeleitete manuelle Aktualisierung	Benutzer starten das Update von ihrem Macintosh-Computer aus.

Agent-Update-Adressen

Standardmäßig laden Agents die Komponenten vom Trend Micro Security (für Mac) Server herunter. Zusätzlich zu den Komponenten erhalten Trend Micro Security (für Mac) Agents beim Update vom Trend Micro Security (für Mac) Server auch aktualisierte Konfigurationsdateien. Agents benötigen diese Konfigurationsdateien, um neue Einstellungen zu übernehmen. Bei jeder Änderung der Einstellungen für Trend Micro Security (für Mac) in der Webkonsole ändern sich auch die Konfigurationsdateien.

Überprüfen Sie, ob der Trend Micro Security (für Mac) Server über die neuesten Komponenten verfügt, bevor Sie die Agents aktualisieren. Informationen dazu, wie Sie

den Trend Micro Security (für Mac) Server aktualisieren, finden Sie unter *Server-Update auf Seite 5-4*.

Sie können einen, mehrere oder alle Agents so konfigurieren, dass sie Komponenten vom Trend Micro ActiveUpdate Server herunterladen, wenn der Trend Micro Security (für Mac) Server nicht verfügbar sein sollte. Weitere Informationen finden Sie unter *Agent-Update-Einstellungen konfigurieren auf Seite 5-10*.



Hinweis

Wenn ein Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Agent-Updates in *Einschränkungen eines reinen IPv6-Agents auf Seite A-3*.

Hinweise und Erinnerungen für Agent-Updates

- Trend Micro Security (für Mac) Agents können auch Proxy-Einstellungen für Updates verwenden. Proxy-Einstellungen werden über die Agent-Konsole konfiguriert.
- Während eines Updates zeigt das Symbol für Trend Micro Security (für Mac) in der Menüleiste von Mac-Computern den laufenden Aktualisierungsvorgang an. Ist ein Upgrade für das Agent-Programm verfügbar, führen die Agents zunächst das Update und dann das Upgrade auf die neueste Programmversion oder den neuesten Build durch. Bis zum Abschluss des Updates können keine Tasks über die Konsole gestartet werden.
- Überprüfen Sie im Übersichtsfenster, ob alle Agents aktualisiert wurden.

Agent-Update-Einstellungen konfigurieren

Detaillierte Erklärungen zu Agent-Updates erhalten Sie unter *Agent-Updates auf Seite 5-8*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.

3. Klicken Sie auf **Einstellungen** > **Einstellungen für Updates**.
4. Aktivieren Sie das Kontrollkästchen, um den Agents den Download von Updates vom Trend Micro ActiveUpdate Server zu erlauben.



Hinweis

Wenn ein Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Agent-Updates in *Einschränkungen eines reinen IPv6-Agents auf Seite A-3*.

5. Konfigurieren Sie die zeitgesteuerten Updates.
   a. Wählen Sie **Zeitgesteuertes Update aktivieren**.
   b. Konfigurieren Sie den Zeitplan.
   c. Geben Sie bei Auswahl von **Täglich** oder **Wöchentlich** die Uhrzeit des Updates und den Zeitraum an, in dem der Trend Micro Security (für Mac) Server die Agents zum Update der Komponenten auffordert. Wenn Sie die Startzeit beispielsweise für 12 Uhr und den Zeitraum mit 2 Stunden festlegen, fordert der Server zwischen 12 und 14 Uhr in zufälligen Abständen alle online geschalteten Agents zum Update auf. Mit dieser Einstellung wird verhindert, dass sich alle Agents gleichzeitig zum festgelegten Zeitpunkt mit dem Server verbinden, damit es zu keiner Überlastung des Servers kommt.
6. Wenn Sie Gruppen oder Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die ausgewählten Gruppen oder Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:
   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf neu zu einer vorhandenen/zukünftigen Gruppe hinzukommende Agents an. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
   - **Nur auf zukünftige Gruppen anwenden**: Wendet Einstellungen nur auf Agents an, die zu zukünftigen Gruppen hinzugefügt wurden. Bei dieser Option werden die Einstellungen nicht auf neue Agents angewendet, die zu einer vorhandenen Gruppe hinzukommen.

Agent-Updates aus dem Übersichtsfenster starten

Informationen zu anderen Agent-Update-Methoden finden Sie unter *Agent-Updates auf Seite 5-8*.

Prozedur

1. Klicken Sie im Hauptmenü auf **Übersicht**.
2. Klicken Sie im Bereich **Update-Status** auf den Link in der Spalte **Nicht aktuell**.

   Die Agent-Struktur wird geöffnet, und es werden alle Agents angezeigt, die aktualisiert werden müssen.
3. Wählen Sie die Agents aus, die Sie aktualisieren möchten.
4. Klicken Sie auf **Tasks** > **Update**.

   Das Update wird auf allen Agents durchgeführt, die die Benachrichtigung erhalten. Auf Mac-Computern zeigt das Symbol für Trend Micro Security (für Mac) in der Menüleiste den laufenden Aktualisierungsvorgang an. Bis zum Abschluss des Updates können keine Tasks über die Konsole gestartet werden.

Agent-Updates aus dem Agent-Verwaltung-Fenster starten

Informationen zu anderen Agent-Update-Methoden finden Sie unter *Agent-Updates auf Seite 5-8*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammdomänensymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Tasks** > **Update**.

Das Update wird auf allen Agents durchgeführt, die die Benachrichtigung erhalten. Auf Mac-Computern zeigt das Symbol für Trend Micro Security (für Mac) in der Menüleiste den laufenden Aktualisierungsvorgang an. Bis zum Abschluss des Updates können keine Tasks über die Konsole gestartet werden.



Kapitel 6

Mac-Computer vor Sicherheitsrisiken schützen

In diesem Kapitel wird beschrieben, wie Sie Computer durch dateibasierte Suchvorgänge vor Sicherheitsrisiken schützen können.

Info über Sicherheitsrisiken

Sicherheitsrisiken umfassen Viren, Malware, Spyware und Grayware. Trend Micro Security (für Mac) Schützt Computer vor Sicherheitsrisiken, indem Dateien durchsucht werden und dann eine spezifische Aktion für jedes entdeckte Sicherheitsrisiko durchgeführt wird. Eine große Anzahl entdeckter Sicherheitsrisiken innerhalb kurzer Zeit deutet auf einen Virenausbruch hin. Durch Anwendung von Ausbruchspräventionsrichtlinien und die Isolierung infizierter Computer, bis keine Bedrohung mehr von ihnen ausgeht, kann Trend Micro Security (für Mac) helfen, die schädlichen Auswirkungen zu begrenzen. Mittels Benachrichtigungen und Protokollen werden Sie ständig über den Verlauf der Sicherheitsrisiken informiert und alarmiert, wenn Sofortmaßnahmen erforderlich sind.

Viren und Malware

Zehntausende von Viren und Malware-Typen sind bereits bekannt, und täglich kommen neue hinzu. Durch Ausnutzen von Schwachstellen in Unternehmensnetzwerken, E-Mail-Systemen und Websites können Computerviren heutzutage verheerende Schäden anrichten.

Trend Micro Security (für Mac) schützt Computer vor folgenden Viren- und Malware-Typen:

VIREN-/MALWARE-TYPEN	BESCHREIBUNG
Scherzprogramm	Ein Scherzprogramm ist ein virenähnliches Programm, das meist die Anzeige auf dem Computerbildschirm verändert.
Trojaner	Ein Trojaner ist ein ausführbares Programm, das sich nicht selbst repliziert, sondern in einem System einnistet und unerwünschte Aktionen auslöst (z. B. Ports für Hacker zugänglich macht). Dieses Programm verschafft sich oft über Trojanerports Zugang zu Computern. Ein bekanntes Beispiel für einen Trojaner ist eine Anwendung, die vorgibt, den betreffenden Computer von Viren zu befreien, obwohl sie in Wirklichkeit den Computer mit Viren infiziert.

Viren-/Malware-Typen	Beschreibung
Virus	Ein Virus ist ein Programm, das sich selbst vervielfältigt. Der Virus muss sich dazu an andere Programmdateien anhängen und wird ausgeführt, sobald das Host-Programm ausgeführt wird. • **Bootvirus**: Diese Virenart infiziert den Bootsektor von Partitionen oder Festplatten. • **Bösartiger Java-Code**: Virencode, der in Java geschrieben oder eingebettet wurde und auf einem beliebigen Betriebssystem ausgeführt werden kann • **Makrovirus**: Diese Virenart ist wie das Makro einer Anwender-Software aufgebaut und verbirgt sich häufig in Dokumenten. • **VBScript-, JavaScript- oder HTML-Virus**: Ein Virus, der sich auf Websites verbirgt und über den Browser heruntergeladen wird • **Wurm**: Ein eigenständig oder in Gruppen auftretendes Programm, das funktionsfähige Kopien von sich selbst oder seinen Segmenten an andere Computer (meist per E-Mail) verteilen kann.
Testvirus:	Ein Testvirus ist eine inaktive Datei, die von Antiviren-Software erkannt wird. Mit Testviren wie dem EICAR-Testskript können Sie die Funktion Ihrer Antiviren-Software überprüfen.
Packer	Packer sind komprimierte und/oder verschlüsselte ausführbare Programme für Windows oder Linux™; häufig handelt es sich dabei um Trojaner. In komprimierter Form ist ein Packer für ein Antiviren-Programm schwieriger zu erkennen.
Wahrscheinlich Virus/Malware	Verdächtige Dateien, die einige Eigenschaften von Viren/Malware aufweisen, werden als dieser Viren-/Malware-Typ kategorisiert. Weitere Informationen über wahrscheinliche Viren/Malware finden Sie in der Trend Micro Online-Viren-Enzyklopädie: http://www.trendmicro.com/vinfo/de/virusencyclo/default.asp
Andere	„Andere" bezieht sich auf die Viren/Malware, die unter keinem der Viren-/Malware-Typen eingestuft wurden.

Spyware und Grayware

Die Begriffe Spyware und Grayware beziehen sich auf Anwendungen oder Dateien, die nicht als Viren oder Malware eingestuft werden, sich aber dennoch negativ auf die Leistung von Computern im Netzwerk auswirken können. Spyware stellt ebenso wie Grayware ein signifikantes Sicherheits-, Vertraulichkeits- und rechtliches Risiko für eine Organisation dar. Häufig führt Spyware/Grayware eine Vielzahl unerwünschter und bedrohlicher Aktionen durch. Dazu zählen das Öffnen lästiger Popup-Fenster, das Aufzeichnen von Tastatureingaben und das Aufdecken von Sicherheitslücken, durch die der Computer angegriffen werden kann.

Trend Micro Security (für Mac) schützt Computer vor folgenden Spyware- und Grayware-Typen:

Spyware-/ Grayware-Typen	Beschreibung
Spyware	Spyware sammelt Daten wie Benutzernamen, Kennwörter, Kreditkartennummern und andere vertrauliche Informationen, um sie an Dritte weiterzuleiten.
Adware	Adware zeigt Werbeschaltungen an und protokolliert Benutzerdaten, beispielsweise das Surfverhalten im Internet, die wiederum zu Werbezwecken genutzt werden.
Dialer	Ein Dialer ändert die Internet-Einstellungen und erzwingt auf dem Client-Computer das Wählen von voreingestellten Telefonnummern. Oft handelt es sich um Pay-per-Call oder internationale Rufnummern, die einem Unternehmen beträchtliche Kosten verursachen können.
Hacker-Tools	Ein Hacker-Tool hilft Hackern, sich Zugriff auf Computer zu verschaffen.
Tools für den Remote-Zugriff	Mit einem Tool für den Remote-Zugriff können Hacker per Fernzugriff in Computer eindringen und diese steuern.
Anwendungen zum Entschlüsseln von Kennwörtern	Mit Hilfe solcher Anwendungen versuchen Hacker, Benutzernamen und Kennwörter zu entschlüsseln.

Spyware-/ Grayware-Typen	Beschreibung
Andere	„Andere" bezieht sich auf die potenziell bösartige Programme, die unter keinem der Spyware-/Grayware-Typen eingestuft wurden.

Suchtypen

Trend Micro Security (für Mac) bietet die folgenden Suchtypen, mit denen Agent-Computer vor Sicherheitsrisiken geschützt werden können;

Suchtyp	Beschreibung
Echtzeitsuche	Beim Empfang, Öffnen, Herunterladen, Kopieren oder Ändern einer Datei auf dem Computer wird diese automatisch durchsucht. Weitere Informationen erhalten Sie unter *Echtzeitsuche auf Seite 6-5*.
Manuelle Suche	Eine vom Benutzer gestartete Suche, bei der eine oder mehrere vom Benutzer angegebene Dateien durchsucht werden. Weitere Informationen erhalten Sie unter *Manuelle Suche auf Seite 6-7*.
Zeitgesteuerte Suche	Dateien auf dem Computer werden automatisch gemäß dem vom Administrator festgelegten Zeitplan durchsucht. Weitere Informationen erhalten Sie unter *Zeitgesteuerte Suche auf Seite 6-8*.
Jetzt durchsuchen	Eine vom Administrator gestartete Suche, bei der Dateien auf einem oder mehreren Zielcomputern durchsucht werden. Weitere Informationen erhalten Sie unter *Jetzt durchsuchen auf Seite 6-9*.

Echtzeitsuche

Die Echtzeitsuche wird kontinuierlich und dauerhaft ausgeführt. Bei jedem Empfang, Öffnen, Herunterladen, Kopieren oder Ändern einer Datei wird diese durch die

Echtzeitsuche nach Sicherheitsrisiken durchsucht. Wenn Trend Micro Security (für Mac) kein Sicherheitsrisiko erkennt, verbleibt die Datei an ihrem Speicherort und Benutzer können darauf zugreifen. Wenn Trend Micro Security (für Mac) ein Sicherheitsrisiko entdeckt, wird eine Nachricht mit dem Namen der infizierten Datei und dem jeweiligen Sicherheitsrisiko angezeigt.

Konfigurieren Sie die Einstellungen der Echtzeitsuche und wenden Sie sie auf einen oder mehrere Agents und Gruppen oder auf alle vom Server verwalteten Agents an.

Einstellungen für Echtzeitsuche konfigurieren

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für Echtzeitsuche**.
4. Folgende Suchkriterien konfigurieren:
    - *Benutzerdefinierte Aktionen für Dateien auf Seite 6-10*
    - *Sucheinstellungen auf Seite 6-12*
5. Klicken Sie auf die Registerkarte **Aktion** , um die Suchaktionen zu konfigurieren, die Trend Micro Security (für Mac) bei entdeckten Sicherheitsrisiken durchführen soll. Details zu den Suchoptionen finden Sie unter *Suchaktionsoptionen und zusätzliche Einstellungen auf Seite 6-15*.
6. Wenn Sie Gruppen oder Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die ausgewählten Gruppen oder Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:
    - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf neu zu einer vorhandenen/zukünftigen Gruppe hinzukommende Agents an. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

- **Nur auf zukünftige Gruppen anwenden**: Wendet Einstellungen nur auf Agents an, die zu zukünftigen Gruppen hinzugefügt wurden. Bei dieser Option werden die Einstellungen nicht auf neue Agents angewendet, die zu einer vorhandenen Gruppe hinzukommen.

Manuelle Suche

Die manuelle Suche wird bei Bedarf gestartet, wenn der Benutzer sie in der Agent-Konsole aktiviert. Die Dauer der Suche hängt von der Anzahl der zu durchsuchenden Dateien und den Hardware-Ressourcen des Mac-Computers ab.

Konfigurieren Sie die Einstellungen der manuellen Suche und wenden Sie sie auf einen oder mehrere Agents und Gruppen oder auf alle vom Server verwalteten Agents an.

Einstellungen für manuelle Suche konfigurieren

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für manuelle Suche**.
4. Folgende Suchkriterien konfigurieren:
   - *Sucheinstellungen auf Seite 6-12*
   - *CPU-Auslastung auf Seite 6-12*
5. Klicken Sie auf die Registerkarte **Aktion** , um die Suchaktionen zu konfigurieren, die Trend Micro Security (für Mac) bei entdeckten Sicherheitsrisiken durchführen soll. Details zu den Suchoptionen finden Sie unter *Suchaktionsoptionen und zusätzliche Einstellungen auf Seite 6-15*.
6. Wenn Sie Gruppen oder Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die ausgewählten Gruppen oder

Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

- **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf neu zu einer vorhandenen/zukünftigen Gruppe hinzukommende Agents an. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
- **Nur auf zukünftige Gruppen anwenden**: Wendet Einstellungen nur auf Agents an, die zu zukünftigen Gruppen hinzugefügt wurden. Bei dieser Option werden die Einstellungen nicht auf neue Agents angewendet, die zu einer vorhandenen Gruppe hinzukommen.

Zeitgesteuerte Suche

Die zeitgesteuerte Suche wird automatisch zum angegebenen Datum und zur angegebenen Uhrzeit ausgeführt. Verwenden Sie die zeitgesteuerte Suche, um die routinemäßige Suche auf dem Agent zu automatisieren und die Verwaltung der Virensuche zu optimieren.

Konfigurieren Sie die Einstellungen der zeitgesteuerten Suche und wenden Sie sie auf einen oder mehrere Agents und Gruppen oder auf alle vom Server verwalteten Agents an.

Einstellungen für zeitgesteuerte Suche konfigurieren

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für zeitgesteuerte Suche**.
4. Aktivieren Sie das Kontrollkästchen, um die zeitgesteuerte Suche zu aktivieren.
5. Folgende Suchkriterien konfigurieren:

- *Zeitplan auf Seite 6-13*
- *Suchziel auf Seite 6-11*
- *Sucheinstellungen auf Seite 6-12*
- *CPU-Auslastung auf Seite 6-12*

6. Klicken Sie auf die Registerkarte **Aktion** , um die Suchaktionen zu konfigurieren, die Trend Micro Security (für Mac) bei entdeckten Sicherheitsrisiken durchführen soll. Details zu den Suchoptionen finden Sie unter *Suchaktionsoptionen und zusätzliche Einstellungen auf Seite 6-15*.

7. Wenn Sie Gruppen oder Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die ausgewählten Gruppen oder Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

    - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf neu zu einer vorhandenen/zukünftigen Gruppe hinzukommende Agents an. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.
    - **Nur auf zukünftige Gruppen anwenden**: Wendet Einstellungen nur auf Agents an, die zu zukünftigen Gruppen hinzugefügt wurden. Bei dieser Option werden die Einstellungen nicht auf neue Agents angewendet, die zu einer vorhandenen Gruppe hinzukommen.

Jetzt durchsuchen

Jetzt durchsuchen wird per Fernzugriff durch einen Administrator für Trend Micro Security (für Mac) über die Webkonsole gestartet und kann auf einem oder mehreren Agent-Computern ausgeführt werden.

Starten Sie Jetzt durchsuchen auf Computern, bei denen Sie eine Vireninfektion vermuten.

Jetzt durchsuchen starten

Vorbereitungen

Jetzt durchsuchen verwendet alle Einstellungen der zeitgesteuerten Suche mit Ausnahme des Zeitplans. Zum Konfigurieren der Einstellungen vor dem Start von Jetzt durchsuchen befolgen Sie die Schritte in *Einstellungen für zeitgesteuerte Suche konfigurieren auf Seite 6-8*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Tasks** > **Jetzt durchsuchen**.

Gemeinsame Einstellungen für alle Suchtypen

Konfigurieren Sie für alle Sucharten drei Einstellungsgruppen: Suchkriterien, Suchausschlüsse und Suchaktionen. Verteilen Sie diese Einstellungen auf einen oder mehrere Agents und Gruppen oder auf alle vom Server verwalteten Agents.

Suchkriterien

Geben Sie an, welche Dateien ein bestimmter Suchtyp durchsuchen soll. Verwenden Sie dafür Dateiattribute wie Dateityp und Dateierweiterung. Geben Sie auch die Bedingungen an, die die Suche auslösen sollen. Konfigurieren Sie z. B. die Echtzeitsuche so, dass jede Datei durchsucht wird, die auf den Computer heruntergeladen wird.

Benutzerdefinierte Aktionen für Dateien

Wählen Sie Aktivitäten für Dateien aus, die die Echtzeitsuche auslösen. Wählen Sie unter folgenden Optionen:

- **Dateien durchsuchen, die erstellt/bearbeitet werden**: Durchsucht Dateien, die dem Computer neu hinzugefügt wurden (z. B. nach dem Herunterladen einer Datei) oder gerade verändert werden.
- **Dateien durchsuchen, die abgefragt werden**: Durchsucht Dateien beim Öffnen.
- **Dateien durchsuchen, die erstellt/bearbeitet und abgefragt werden**

Beispiel, falls die dritte Option aktiviert wird: Wird eine neue Datei auf den Computer heruntergeladen, wird sie durchsucht. Wenn kein Sicherheitsrisiko entdeckt wird, bleibt sie an ihrem aktuellen Speicherort. Dieselbe Datei wird erneut durchsucht, wenn sie geöffnet wird und bevor etwaige Änderungen daran gespeichert werden.

Suchziel

Wählen Sie unter folgenden Optionen:

- **Alle durchsuchbaren Dateien**: Alle Dateien durchsuchen
- **Von IntelliScan durchsuchte Dateitypen**: Durchsucht nur Dateien, die potenziell bösartigen Code enthalten, selbst wenn dieser sich hinter einer scheinbar harmlosen Erweiterung verbirgt. Weitere Informationen finden Sie unter *IntelliScan auf Seite B-2*.
- **Datei- oder Ordnername mit vollständigem Pfad**: Durchsucht nur die angegebene(n) Datei(en) in einem bestimmten Ordner.

  1. Geben Sie einen vollständigen Dateipfad oder einen Verzeichnispfad ein und klicken Sie auf **Hinzufügen**.
     - Beispiel eines vollständigen Dateipfads: `/Benutzer/Benutzername/temp.zip`
     - Beispiel eines Verzeichnispfads: `/Benutzer/Benutzername`
  2. Zum Löschen eines Verzeichnispfads oder eines vollständigen Pfads wählen Sie ihn aus und klicken auf **Entfernen**.

Sucheinstellungen

Trend Micro Security (für Mac) kann einzelne Dateien innerhalb komprimierter Dateien durchsuchen. Trend Micro Security (für Mac) unterstützt die folgenden Komprimierungstypen:

ERWEITERUNG	TYP
.zip	Mit Pkzip erstelltes Archiv
.rar	Mit RAR erstelltes Archiv
.tar	Mit Tar erstelltes Archiv
.arj	ARJ-komprimiertes Archiv
.hqx	BINHEX
.gz; .gzip	Gnu ZIP
.Z	LZW/16-Bit-komprimiert
.bin	MacBinary
.cab	Microsoft Kabinettdatei
Microsoft komprimiert/MSCOMP	
.eml; .mht	MIME
.td0	Teledisk Format
.bz2	Mit Unix BZ2 Bzip komprimierte Datei
.uu	UUEncode
.ace	WinAce

CPU-Auslastung

Trend Micro Security (für Mac) kann nach dem Durchsuchen einer Datei und vor dem Durchsuchen der nächsten eine Pause einlegen. Diese Einstellung wird für die manuelle Suche, die zeitgesteuerte Suche und Jetzt durchsuchen verwendet.

Wählen Sie unter folgenden Optionen:

- **Hoch**: Keine Pause zwischen den einzelnen Suchläufen
- **Niedrig**: Pause zwischen den einzelnen Dateisuchläufen

Zeitplan

Stellen Sie ein, wie oft (täglich, wöchentlich oder monatlich) und wann die zeitgesteuerte Suche durchgeführt werden soll.

Wenn Sie für die monatliche zeitgesteuerte Suche den 29., 30. oder 31. Tag des Monats ausgewählt haben, dieser Tag im betreffenden Monat jedoch nicht vorkommt, führt Trend Micro Security (für Mac) die zeitgesteuerte Suche am letzten Tag des Monats durch.

Suchaktionen

Geben Sie die Aktion an, die Trend Micro Security (für Mac) durchführen soll, wenn ein bestimmter Suchtyp ein Sicherheitsrisiko erkannt hat.

Die Aktion, die von Trend Micro Security (für Mac) ausgeführt wird, ist abhängig vom Suchtyp, der das Sicherheitsrisiko erkannt hat. Wenn beispielsweise bei der manuellen Suche (Suchtyp) ein Sicherheitsrisiko von Trend Micro Security (für Mac) erkannt wird, wird die infizierte Datei gesäubert (Aktion).

Trend Micro Security (für Mac) kann die folgenden Aktionen gegen Sicherheitsrisiken durchführen:

SUCHAKTION	DETAILS
Löschen	Trend Micro Security (für Mac) entfernt die infizierte Datei vom Computer.

SUCHAKTION	DETAILS
Quarantäne	Die infizierte Datei wird von Trend Micro Security (für Mac) umbenannt und in das Quarantäneverzeichnis des Agent-Computers in <*Agent-Installationsordner*>`/common/lib/vsapi/quarantine` verschoben. Nachdem die Datei in das Quarantäneverzeichnis verschoben wurde, kann Trend Micro Security (für Mac) weitere Aktionen für diese Datei durchführen, je nachdem, welche Aktion vom Benutzer angegeben wurden. Trend Micro Security (für Mac) kann die Datei säubern, löschen oder wiederherstellen. Die Datei wiederherzustellen bedeutet, dass sie an ihren ursprünglichen Speicherort zurückverschoben wird, ohne dass irgendeine Aktion ausgeführt wird. Benutzer können eine Datei wiederherstellen, wenn sie sich als unbedenklich herausstellt. Eine Datei zu säubern bedeutet, dass das Sicherheitsrisiko von der Datei in der Quarantäne entfernt wird und sie nach erfolgreicher Säuberung an ihren ursprünglichen Speicherort zurückverschoben wird.
Säubern	Trend Micro Security (für Mac) entfernt das Sicherheitsrisiko aus einer infizierten Datei und ermöglicht dann erst den Zugriff auf die Datei. Lässt sich die Datei nicht säubern, führt Trend Micro Security (für Mac) zusätzlich eine der folgenden Aktionen aus: Quarantäne, Löschen oder Übergehen. Zum Konfigurieren der zweiten Aktion gehen Sie zu **Agent-Verwaltung** > **Einstellungen** > **{Suchtyp}** und klicken auf die Registerkarte **Aktion**.

SUCHAKTION	DETAILS
Übergehen	Trend Micro Security (für Mac) führt keine Aktion an der infizierten Datei aus. Das erkannte Sicherheitsrisiko wird jedoch in den Protokolldateien verzeichnet. Die Datei wird nicht verschoben. Trend Micro Security (für Mac) führt bei Dateien mit Infektionen des Typs „Wahrscheinlich Virus/Malware“ stets die Aktion „Übergehen“ aus, um das Risiko von Fehlalarmen zu verringern. Wenn weitere Analysen bestätigen, dass „Wahrscheinlich Virus/Malware“ ein tatsächliches Sicherheitsrisiko darstellt, wird ein neues Pattern veröffentlicht, damit Trend Micro Security (für Mac) die entsprechende Suchaktion durchführen kann. Wenn sich wahrscheinliche Viren/ Malware als unbedenklich herausstellen, werden diese nicht mehr entdeckt. Zum Beispiel: Trend Micro Security (für Mac) entdeckt in der Datei „123.pdf“ das Sicherheitsrisiko „x_wahrscheinlicher_Virus“ und führt zum Zeitpunkt der Erkennung keine Aktion aus. Trend Micro bestätigt anschließend, dass „x_wahrscheinlicher_Virus“ ein Trojaner ist und veröffentlicht eine neue Version des Viren-Patterns. Nach dem Laden der neuen Pattern-Version erkennt Trend Micro Security (für Mac) „x_wahrscheinlicher_Virus“ als Trojaner und löscht „123.pdf“, wenn für Trojaner die Aktion „Löschen“ festgelegt wurde.

Suchaktionsoptionen und zusätzliche Einstellungen

Wählen Sie für die Einstellung der Suchaktion unter folgenden Optionen:

OPTION	DETAILS
ActiveAction verwenden	In ActiveAction sind mehrere vorkonfigurierte Aktionen für die Suche nach unterschiedlichen Arten von Sicherheitsrisiken zusammengefasst. Trend Micro empfiehlt die Verwendung von ActiveAction, wenn Sie nicht genau wissen, welche Suchaktion sich für einen bestimmten Typ von Sicherheitsrisiko am besten eignet. Die ActiveAction-Einstellungen werden in den Pattern-Dateien ständig aktualisiert, um Computer gegen die neuesten Sicherheitsrisiken und die neuesten Angriffsmethoden zu schützen.

Option	Details
Die gleiche Aktion für alle Typen von Sicherheitsrisiken verwenden	Wählen Sie diese Option, wenn dieselbe Aktion für alle Typen von Sicherheitsrisiken außer für wahrscheinliche Viren/Malware durchgeführt werden soll. Beim Typ „Wahrscheinlich Virus/Malware" erfolgt stets die Aktion „Übergehen". Wenn Sie „Säubern" als erste Aktion auswählen, geben Sie eine zweite Aktion an, die Trend Micro Security (für Mac) durchführen soll, falls das Säubern fehlschlägt. Nur wenn die erste Aktion „Säubern" ist, ist eine zweite Aktion einstellbar. Details zu den Suchoptionen finden Sie unter *Suchaktionen auf Seite 6-13*.

Zusätzliche Einstellungen für Echtzeitsuche

Einstellung	Details
Bei Erkennung eines Sicherheitsrisikos Benachrichtigung anzeigen	Erkennt Trend Micro Security (für Mac) während der Echtzeitsuche ein Sicherheitsrisiko, kann dem Benutzer eine entsprechende Benachrichtigung angezeigt werden.

Zeitgesteuerte Suche – Berechtigungen

Wenn auf dem Mac-Computer die zeitgesteuerte Suche aktiviert ist, kann sie vom Benutzer übersprungen und angehalten werden.

BERECHTIGUNG	DETAILS
Zeitgesteuerte Suche verschieben	Ein Benutzer mit der Berechtigung „Zeitgesteuerte Suche verschieben“ darf folgende Aktionen durchführen: • Der Benutzer kann die zeitgesteuerte Suche vor der Ausführung verschieben und die Dauer der Verschiebung angeben. Ein zeitgesteuerte Suche kann nur einmal verschoben werden. • Wenn die zeitgesteuerte Suche bereits ausgeführt wird, kann sie durch den Benutzer angehalten und zu einem späteren Zeitpunkt neu gestartet werden. Anschließend gibt der Benutzer an, wie viel Zeit bis zum Neustart der Suche verstreichen soll. Wenn die Suche neu startet, werden alle vorher durchsuchten Dateien erneut durchsucht. Die zeitgesteuerte Suche kann nur einmal angehalten und neu gestartet werden. Der Benutzer kann die Anzahl der Stunden und Minuten für folgende Einstellungen angeben: • die maximale Dauer der Verschiebung • die maximalen Zeit, die bis zum Neustart der Suche verstreichen soll
Zeitgesteuerte Suche überspringen und anhalten	Mit dieser Berechtigung darf ein Benutzer folgende Aktionen durchführen: • zeitgesteuerte Suche vor der Ausführung überspringen • zeitgesteuerte Suche während der Ausführung anhalten

Zusätzliche Einstellungen für zeitgesteuerte Suche

EINSTELLUNG	DETAILS
Vor Beginn der zeitgesteuerten Suche Benachrichtigung anzeigen	Wenn Sie diese Option aktivieren, wird ein paar Minuten vor Beginn der zeitgesteuerten Suche eine Benachrichtigung auf dem betreffenden Mac-Computer angezeigt. Darin erhalten die Benutzer Auskunft über den Zeitplan (Datum und Uhrzeit) und ihre Berechtigungen im Zusammenhang mit der zeitgesteuerten Suche, etwa ob sie das Recht haben, sie zu verschieben, zu überspringen oder anzuhalten. Sie können die Dauer der Anzeige der Benachrichtigung in Minuten festlegen.
Zeitgesteuerte Suche automatisch anhalten, wenn Suche länger als __ Stunden und __ Minuten dauert	Der Agent bricht die Suche ab, sobald der angegebene Zeitraum erreicht wird, auch wenn die Suche noch nicht vollständig ist. Der Agent informiert den Benutzer umgehend über etwaige bei der Suche erkannte Sicherheitsrisiken.

Suchausschlüsse

Konfigurieren Sie die Suchausschlüsse, um die Suchleistung zu verbessern und bekannte Dateien zu überspringen, die keinen Schaden anrichten können. Während ein bestimmter Suchtyp ausgeführt wird, überprüft Trend Micro Security (für Mac) die Ausschlussliste, um die Dateien zu bestimmen, die von der Suche ausgeschlossen werden.

AUSSCHLUSSLISTE	DETAILS
Dateien	Trend Micro Security (für Mac) wird eine Datei nicht durchsuchen, wenn: • die Datei sich im Verzeichnispfad befindet, der in der Ausschlussliste angegeben ist • die Datei dem vollständigen Dateipfad (Verzeichnispfad und Dateiname) entspricht, der in der Ausschlussliste angegeben ist

AUSSCHLUSSLISTE	DETAILS
Dateierweiterungen	Trend Micro Security (für Mac) wird eine Datei nicht durchsuchen, wenn ihre Erweiterung einer der Erweiterungen in der Ausschlussliste entspricht.

Ausschlusslisten für die Suche konfigurieren

Details zu Ausschlusslisten für die Virensuche finden Sie unter *Suchausschlüsse auf Seite 6-18*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol (), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für den Suchausschluss**.
4. Aktivieren Sie das Kontrollkästchen, um den Suchausschluss zu aktivieren.
5. So konfigurieren Sie die **Ausschlussliste für Virensuche (Dateien)**

   a. Geben Sie einen vollständigen Dateipfad oder einen Verzeichnispfad ein und klicken Sie auf **Hinzufügen**.

      Erinnerung:

      - Die Eingabe nur eines Dateinamens ist nicht zulässig.
      - Es können maximal 64 Pfade angegeben werden. Beispiele erhalten Sie in der folgenden Tabelle.

PFAD	DETAILS	BEISPIELE

Vollständiger Dateipfad	Schließt eine bestimmte Datei auf dem Computer aus.	• Beispiel 1:
		`/file.log`
		• Beispiel 2:
		`/System/file.log`

Verzeichnispfad	Schließt alle Dateien in einem bestimmten Ordner und dessen Unterordnern aus.	• Beispiel 1: `/System/` Beispiele für aus Suchvorgängen ausgeschlossene Dateien: • `/System/file.log` • `/System/Library/file.log` Beispiele für Dateien, die durchsucht werden: • `/Applications/file.log` • Beispiel 2: `/System/Library` Beispiele für aus Suchvorgängen ausgeschlossene Dateien: • `/System/Library/file.log` • `/System/Library/Filters/file.log` Beispiele für Dateien, die durchsucht werden: • `/System/file.log`

- Sie können statt Ordnernamen auch ein Sternchen (*) als Platzhalterzeichen verwenden.

Beispiele erhalten Sie in der folgenden Tabelle.

PFAD	BEISPIELE FÜR DIE VERWENDUNG VON PLATZHALTERZEICHEN
Vollständiger Dateipfad	`/Users/Mac/*/file.log` Beispiele für aus Suchvorgängen ausgeschlossene Dateien: • `/Users/Mac/Desktop/file.log` • `/Users/Mac/Movies/file.log` Beispiele für Dateien, die durchsucht werden: • `/Users/file.log` • `/Users/Mac/file.log`

PFAD	BEISPIELE FÜR DIE VERWENDUNG VON PLATZHALTERZEICHEN

Verzeichnispfad	• Beispiel 1:
	`/Users/Mac/*`
	Beispiele für aus Suchvorgängen ausgeschlossene Dateien:
	• `/Users/Mac/doc.html`
	• `/Users/Mac/Documents/doc.html`
	• `/Users/Mac/Documents/Pics/pic.jpg`
	Beispiele für Dateien, die durchsucht werden:
	• `/Users/doc.html`
	• Beispiel 2:
	`/*/Components`
	Beispiele für aus Suchvorgängen ausgeschlossene Dateien:
	• `/Users/Components/file.log`
	• `/System/Components/file.log`
	Beispiele für Dateien, die durchsucht werden:
	• `/file.log`
	• `/Users/file.log`
	• `/System/Files/file.log`

- Teilweise Übereinstimmungen mit Ordnernamen sind nicht zulässig. So ist es beispielsweise nicht möglich, durch Eingabe von `/Users/*user/temp` Dateien in Ordnern auszuschließen, deren Namen auf `user` enden, etwa `end_user` oder `new_user`.

b. Um einen Pfad zu löschen, wählen Sie ihn aus und klicken Sie auf **Entfernen**.

6. So konfigurieren Sie die **Ausschlussliste für Virensuche (Dateierweiterungen)**

a. Geben Sie eine Dateierweiterung ohne Punkt (.) ein und klicken Sie auf **Hinzufügen**. Geben Sie z. B. `pdf` ein. Es können maximal 64 Dateierweiterungen angegeben werden.

b. Um eine Erweiterung zu löschen, wählen Sie sie aus und klicken auf **Entfernen**.

7. Wenn Sie Gruppen oder Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die ausgewählten Gruppen oder Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf neu zu einer vorhandenen/zukünftigen Gruppe hinzukommende Agents an. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

   - **Nur auf zukünftige Gruppen anwenden**: Wendet Einstellungen nur auf Agents an, die zu zukünftigen Gruppen hinzugefügt wurden. Bei dieser Option werden die Einstellungen nicht auf neue Agents angewendet, die zu einer vorhandenen Gruppe hinzukommen.

Zwischenspeicher-Einstellungen für Suchen

Bei jeder Suche prüft der Agent den **Zwischenspeicher für geänderte Dateien**, um zu ermitteln, ob eine Datei seit dem letzten Start des Agent geändert wurde.

- Ist dies der Fall, durchsucht der Agent die Datei und fügt Sie dem **Zwischenspeicher für durchsuchte Dateien** hinzu.

- Wurde die Datei nicht geändert, sieht der Agent nach, ob sich die Datei im Zwischenspeicher für durchsuchte Dateien befindet.

  - Wenn sie dort vorhanden ist, wird sie bei der Suche übersprungen.

  - Wenn sie sich nicht im Zwischenspeicher für durchsuchte Dateien befindet, sieht der Agent im **Zwischenspeicher für genehmigte Dateien** nach.



Hinweis

Der Zwischenspeicher für genehmigte Dateien enthält alle Dateien, die von Trend Micro Security (für Mac) für vertrauenswürdig befunden werden. Vertrauenswürdige Dateien sind entweder Dateien, die von aufeinanderfolgenden Versionen des Pattern durchsucht und jedes Mal für frei von Bedrohungen befunden wurden, oder bedrohungsfreie Dateien, die seit längerem nicht mehr geändert wurden.

- Wenn die Datei im Zwischenspeicher für genehmigte Dateien vorhanden ist, wird sie bei der Suche übersprungen.
- Ist dies nicht der Fall, durchsucht der Agent die Datei und fügt Sie dem Zwischenspeicher für durchsuchte Dateien hinzu.

Bei jeder Aktualisierung der Such-Engine bzw. des Such-Pattern werden alle oder zumindest einige der Zwischenspeicher geleert.

Wenn Suchvorgänge häufig ausgeführt werden und sich bereits viele Dateien in den Zwischenspeichern befinden, reduziert sich die Suchzeit erheblich.

Wenn Sie die Suche nur selten ausführen, deaktivieren Sie die Zwischenspeicher, so dass bei jeder Suche alle Dateien auf Bedrohungen durchsucht werden können.

Zwischenspeicher-Einstellungen für Suchen konfigurieren

Details zum Zwischenspeicher der On-Demand-Suche finden Sie unter *Zwischenspeicher-Einstellungen für Suchen auf Seite 6-23*.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Zwischenspeicher-Einstellungen für Suchen**.
4. Wählen Sie **Zwischenspeicher der On-Demand-Suche aktivieren**.

5. Wenn Sie Gruppen oder Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die ausgewählten Gruppen oder Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

    - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf neu zu einer vorhandenen/zukünftigen Gruppe hinzukommende Agents an. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

    - **Nur auf zukünftige Gruppen anwenden**: Wendet Einstellungen nur auf Agents an, die zu zukünftigen Gruppen hinzugefügt wurden. Bei dieser Option werden die Einstellungen nicht auf neue Agents angewendet, die zu einer vorhandenen Gruppe hinzukommen.

Benachrichtigungen und Protokolle für Sicherheitsrisiken

Trend Micro Security (für Mac) umfasst zahlreiche Standardbenachrichtigungen, die Sie und andere Administratoren für Trend Micro Security (für Mac) erhalten, wenn Sicherheitsrisiken oder Virenausbrüche erkannt werden.

Trend Micro Security (für Mac) erstellt Protokolldateien, wenn Sicherheitsrisiken entdeckt werden.

Einstellungen der Administratorbenachrichtigungen konfigurieren

Wenn Sicherheitsrisiken erkannt werden oder ein Ausbruch auftritt, erhalten Administratoren für Trend Micro Security (für Mac) eine Benachrichtigung per E-Mail.

Prozedur

1. Gehen Sie zu **Benachrichtigungen** > **Allgemeine Einstellungen**.

2. Geben Sie im Feld **SMTP-Server** eine IPv4- bzw. IPv6-Adresse oder einen Computernamen ein.

3. Geben Sie eine Portnummer zwischen 1 und 65535 ein.

4. Geben Sie im Feld **Von** die E-Mail-Adresse des Absenders ein.

5. Klicken Sie auf **Speichern**.

Benachrichtigungen bei Sicherheitsrisiken für Administratoren konfigurieren

Sie können Trend Micro Security (für Mac) so konfigurieren, dass entweder bei jedem entdeckten Sicherheitsrisiko eine Benachrichtigung gesendet werden soll oder nur dann, wenn die Aktion für das entdeckte Sicherheitsrisiko fehlschlägt und Ihr Eingreifen erfordert.

Sie können sich Benachrichtigungen per E-Mail zusenden lassen. Konfigurieren Sie die Einstellungen der Administratorbenachrichtigungen so, dass Trend Micro Security (für Mac) Benachrichtigungen per E-Mail versenden kann. Weitere Informationen finden Sie unter *Einstellungen der Administratorbenachrichtigungen konfigurieren auf Seite 6-25*.

Prozedur

1. Gehen Sie zu **Benachrichtigungen** > **Standardbenachrichtigungen**.

2. Geben Sie auf der Registerkarte **Kriterien** an, ob Benachrichtigungen jedes Mal gesendet werden sollen, wenn Trend Micro Security (für Mac) ein Sicherheitsrisiko entdeckt wird, oder nur dann, wenn die Aktion an den Sicherheitsrisiken fehlschlägt.

3. Klicken Sie auf **Speichern**.

4. Auf der Registerkarte **E-Mail**:

    a. Aktivieren Sie das Versenden von Benachrichtigungen per E-Mail.

    b. Geben Sie die die E-Mail-Empfänger an, und akzeptieren oder ändern Sie den Standardbetreff.

Daten im Feld **Nachricht** werden mit Hilfe von Token-Variablen dargestellt.

VARIABLE	BESCHREIBUNG
%v	Name des Sicherheitsrisikos
%s	Der Computer, auf dem das Sicherheitsrisiko erkannt wurde
%m	Agent-Strukturgruppe des Computers
%p	Fundort des Sicherheitsrisikos
%y	Datum und Uhrzeit der Erkennung

5. Klicken Sie auf **Speichern**.

Ausbruchsbenachrichtigungen für Administratoren konfigurieren

Ausbrüche werden auf Grundlage der Anzahl von Sicherheitsrisiken definiert, die in einem bestimmten Zeitraum entdeckt wurden. Nach Festlegung der Ausbruchskriterien konfigurieren Sie Trend Micro Security (für Mac) so, dass Sie und andere Administratoren für Trend Micro Security (für Mac) bei einem Ausbruch benachrichtigt werden, um sofort eingreifen zu können.

Sie können sich Benachrichtigungen per E-Mail zusenden lassen. Konfigurieren Sie die Einstellungen der Administratorbenachrichtigungen so, dass Trend Micro Security (für Mac) Benachrichtigungen per E-Mail versenden kann. Weitere Informationen finden Sie unter *Einstellungen der Administratorbenachrichtigungen konfigurieren auf Seite 6-25*.

Prozedur

1. Gehen Sie zu **Benachrichtigungen** > **Ausbruchsbenachrichtigungen**.

2. Geben Sie auf der Registerkarte **Kriterien** Folgendes an:

    - Anzahl der eindeutigen Quellen von Sicherheitsrisiken

    - Anzahl der Funde

- Entdeckungszeitraum



Tipp

Trend Micro empfiehlt, die Standardeinstellungen in diesem Fenster zu übernehmen.

Trend Micro Security (für Mac) löst einen Virenausbruchalarm aus und sendet eine Benachrichtigung, wenn die festgelegte Anzahl von Entdeckungen überschritten wird. Bei einer festgelegten Anzahl von beispielsweise 100 Entdeckungen sendet Trend Micro Security (für Mac) beim 101. erkannten Sicherheitsrisiko eine Benachrichtigung.

3. Klicken Sie auf **Speichern**.
4. Auf der Registerkarte **E-Mail**:
   a. Aktivieren Sie das Versenden von Benachrichtigungen per E-Mail.
   b. Geben Sie die die E-Mail-Empfänger an, und akzeptieren oder ändern Sie den Standardbetreff.

   Daten im Feld **Nachricht** werden mit Hilfe von Token-Variablen dargestellt.

VARIABLE	BESCHREIBUNG
%CV	Gesamtzahl aller entdeckten Sicherheitsrisiken
%CC	Gesamtzahl aller Computer mit Sicherheitsrisiken

5. Wählen Sie die zusätzlichen Informationen aus, die in der E-Mail enthalten sein sollen. Es können Agent-/Gruppenname, Name des Sicherheitsrisikos, Pfad und infizierte Datei, Datum und Uhrzeit der Entdeckung und das Suchergebnis ausgewählt werden.
6. Klicken Sie auf **Speichern**.

Sicherheitsrisiko-Protokolle anzeigen

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Protokolle** > **Sicherheitsrisiko-Protokolle**.
4. Legen Sie die Protokollkriterien fest, und klicken Sie auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein. Protokolle enthalten die folgenden Informationen:
    - Datum und Uhrzeit des Fundes des Sicherheitsrisikos
    - Computer mit Sicherheitsrisiko
    - Name des Sicherheitsrisikos
    - Quelle des Sicherheitsrisikos
    - Suchtyp, der das Sicherheitsrisiko entdeckt hat
    - Suchergebnisse, die angeben, ob Suchaktionen erfolgreich ausgeführt wurden; Details zu den Suchergebnissen finden Sie unter *Suchergebnis auf Seite 6-30*.
    - Betriebssystem
6. Wenn Sie das Protokoll als komma-separierte Datei im CSV-Format speichern möchten, klicken Sie auf **Exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.



Hinweis

Falls Sie eine große Anzahl an Protokollen exportieren, warten Sie bis der Export abgeschlossen ist. Wenn Sie die Seite schließen, bevor der Export abgeschlossen ist, wird die CSV-Datei nicht erzeugt.

Nächste Maßnahme

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell oder nach einem festgelegten Zeitplan. Weitere Informationen zur Verwaltung von Protokollen finden Sie unter *Protokolle verwalten auf Seite 8-5*.

Suchergebnis

In den Viren-/Malware-Protokollen werden die folgenden Suchergebnisse angezeigt:

- **Gelöscht**
    - Die erste Aktion ist Löschen, und die infizierte Datei wurde gelöscht.
    - Die erste Aktion ist Säubern, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist Löschen, und die infizierte Datei wurde gelöscht.
- **In Quarantäne verschoben**
    - Die erste Aktion ist Quarantäne, und die infizierte Datei wurde in die Quarantäne verschoben.
    - Die erste Aktion ist Säubern, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist Quarantäne, und die infizierte Datei wurde in die Quarantäne verschoben.
- **Gesäubert**

    Eine infizierte Datei wurde gesäubert.
- **Übergangen**
    - Die erste Aktion ist Übergehen. Trend Micro Security (für Mac) hat keine Aktion an der infizierten Datei durchgeführt.
    - Die erste Aktion ist Säubern, aber die Säuberung ist fehlgeschlagen. Die zweite Aktion ist Übergehen, und Trend Micro Security (für Mac) hat demnach keine Aktion an der infizierten Datei durchgeführt.
- **Datei konnte nicht gesäubert oder in Quarantäne verschoben werden**

    Die erste Aktion ist Säubern. Die zweite Aktion ist Quarantäne, und beide Aktionen sind fehlgeschlagen.

Lösung: Weitere Informationen finden Sie unter „Datei konnte nicht in Quarantäne verschoben werden“ weiter unten.

- **Datei konnte nicht gesäubert oder gelöscht werden**

  Die erste Aktion ist Säubern. Die zweite Aktion ist Löschen, und beide Aktionen sind fehlgeschlagen.

  Lösung: Weitere Informationen finden Sie unter „Datei konnte nicht gelöscht werden“ weiter unten.

- **Datei konnte nicht in Quarantäne verschoben werden**

  Die infizierte Datei wird möglicherweise von einer anderen Anwendung gesperrt, gerade ausgeführt oder befindet sich auf einer CD. Trend Micro Security (für Mac) verschiebt die Datei in Quarantäne, nachdem sie wieder verfügbar ist oder ausgeführt wurde.

  Lösung

  Bei infizierten Dateien auf einer CD empfiehlt es sich, die CD nicht zu verwenden, da der Virus auf andere Computer im Netzwerk übertragen werden könnte.

- **Datei konnte nicht gelöscht werden**

  Die infizierte Datei wird möglicherweise von einer anderen Anwendung gesperrt, gerade ausgeführt oder befindet sich auf einer CD. Trend Micro Security (für Mac) löscht die Datei, nachdem sie wieder verfügbar ist oder ausgeführt wurde.

  Lösung

  Bei infizierten Dateien auf einer CD empfiehlt es sich, die CD nicht zu verwenden, da der Virus auf andere Computer im Netzwerk übertragen werden könnte.

- **Die Datei konnte nicht gesäubert werden**

  Die Säuberung der Datei ist möglicherweise nicht durchführbar. Weitere Informationen finden Sie unter *Dateien, die nicht gesäubert werden können auf Seite B-2*.



Kapitel 7

Mac-Computer vor webbasierten Angriffen schützen

In diesem Kapitel werden webbasierte Bedrohungen und die damit verbundenen Schutzfunktionen in Trend Micro Security (für Mac) für Netzwerke und Computer beschrieben.

Internetbedrohungen

Als Internetbedrohungen zählen vielfältige Sicherheitsrisiken, die ihren Ursprung im Internet haben. Sie setzen auf raffinierte Methoden und kombinierte Dateien und Techniken anstelle isolierter Infektionswege. Beispielsweise ändern die Urheber von Internetbedrohungen regelmäßig die Version oder die verwendete Variante. Da sich die Internetbedrohung eher an einem festen Speicherort auf einer Website und nicht auf einem infizierten Computer befindet, wird der Code ständig verändert, um einer Entdeckung zu entgehen.

Personen, die in der Vergangenheit als Hacker, Virenautoren, Spammer und Spyware-Hersteller bezeichnet wurden, werden seit einigen Jahren unter der Bezeichnung Cyberkriminelle zusammengefasst. Internet-Bedrohungen helfen diesen Personen eines von zwei Zielen zu verfolgen. Eines dieser Ziele ist es, Informationen zu stehlen, um sie anschließend zu verkaufen. Das Ergebnis ist die Preisgabe vertraulicher Informationen in Form von Identitätsverlust. Infizierte Computer können außerdem als Überträger für Phishing-Angriffe eingesetzt oder anderweitig zur Informationsbeschaffung missbraucht werden. Unter anderem hat diese Bedrohung das Potenzial, das Misstrauen gegenüber E-Commerce zu verstärken und so das für Transaktionen im Internet notwendige Vertrauen zu zerstören. Das zweite Ziel ist die Nutzung der Rechenleistung eines fremden Computers für profitorientierte Aktivitäten. Solche Aktivitäten können das Versenden von Spam, Erpressungsversuche in Form verteilter Denial-of-Service-Attacken oder Pay-per-Click-Aktivitäten sein.

Web Reputation

Trend Micro Security (für Mac) nutzt die umfangreichen Web Security-Datenbanken von Trend Micro, um die Reputation von Websites zu überprüfen, auf die ein Benutzer zugreifen möchte. Die Reputation einer Website wird mit einer spezifischen, auf dem jeweiligen Computer gültigen Web-Reputation-Richtlinie abgeglichen. Abhängig von dieser Richtlinie erlaubt oder sperrt Trend Micro Security (für Mac) den Zugriff auf die Website. Die Richtlinien gelten jeweils anhand des Standorts des betreffenden Agents.



Hinweis

Diese Funktion unterstützt die neuesten, ab April 2014 veröffentlichten Versionen der Browser Safari™, Mozilla™ Firefox™ und Google Chrome™.

Einstellungen für Web Reputation konfigurieren

Zu den Einstellungen für Web Reputation zählen Web-Reputation-Richtlinien, die bestimmen, ob Trend Micro Security (für Mac) den Zugriff auf eine bestimmte Website zulässt oder sperrt. Um zu ermitteln, welche Richtlinie angewendet werden soll, überprüft Trend Micro Security (für Mac) den Standort des betreffenden Agent. Der Agent-Standort gilt als „intern", wenn eine Verbindung zum Trend Micro Security (für Mac) Server hergestellt werden kann. Andernfalls gilt der Agent-Standort als „extern".

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Einstellungen** > **Einstellungen für Web Reputation**.
4. So konfigurieren Sie eine Richtlinie für externe Agents
    a. Klicken Sie auf die Registerkarte **Externe Agents**.
    b. Wählen Sie **Web-Reputation-Richtlinie aktivieren**.

    Wenn die Richtlinie aktiviert ist, senden interne Agents Web-Reputation-Abfragen an das Smart Protection Network.



Hinweis

Wenn ein Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Web-Reputation-Abfragen in *Einschränkungen eines reinen IPv6-Agents auf Seite A-3*.

c. Wählen Sie aus den vorhandenen Web-Reputation-Sicherheitsstufen eine der folgenden aus: **Hoch**, **Mittel** oder **Niedrig**



Hinweis

Die Sicherheitsstufen legen fest, ob Trend Micro Security (für Mac) den Zugriff auf eine URL zulässt oder sperrt. Wenn beispielsweise die Sicherheitsstufe auf Niedrig festgelegt ist, sperrt Trend Micro Security (für Mac) nur URLs, die bekannte Internetbedrohungen darstellen. Bei einer Erhöhung der Sicherheitsstufe verbessert sich die Erkennungsrate von Internetbedrohungen, doch steigt gleichzeitig auch die Wahrscheinlichkeit von Fehlalarmen.

---

d. Um Web-Reputation-Feedback anzugeben, klicken Sie auf die entsprechende URL. In einem Browserfenster wird das Web-Reputation-Hilfesystem von Trend Micro geöffnet.

5. So konfigurieren Sie eine Richtlinie für interne Agents

a. Klicken Sie auf die Registerkarte **Interne Agents**.

b. Wählen Sie **Web-Reputation-Richtlinie aktivieren**.

Wenn die Richtlinie aktiviert ist, senden interne Agents Web-Reputation-Abfragen andas Smart Protection Network.



Hinweis

Wenn ein Agent ausschließlich eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Web-Reputation-Abfragen in *Einschränkungen eines reinen IPv6-Agents auf Seite A-3*.

---

c. Wählen Sie aus den vorhandenen Web-Reputation-Sicherheitsstufen eine der folgenden aus: **Hoch**, **Mittel** oder **Niedrig**



Hinweis

Die Sicherheitsstufen legen fest, ob Trend Micro Security (für Mac) den Zugriff auf eine URL zulässt oder sperrt. Wenn beispielsweise die Sicherheitsstufe auf Niedrig festgelegt ist, sperrt Trend Micro Security (für Mac) nur URLs, die bekannte Internetbedrohungen darstellen. Bei einer Erhöhung der Sicherheitsstufe verbessert sich die Erkennungsrate von Internetbedrohungen, doch steigt gleichzeitig auch die Wahrscheinlichkeit von Fehlalarmen.

Unabhängig von der Sicherheitsstufe sperren die Agents keine nicht getesteten Websites.

d. Um Web-Reputation-Feedback anzugeben, klicken Sie auf die entsprechende URL. In einem Browserfenster wird das Web-Reputation-Hilfesystem von Trend Micro geöffnet.

e. Bestimmen Sie, ob die Agents Web-Reputation-Protokolle an den Server senden sollen. Dies ist sinnvoll, wenn Sie die von Trend Micro Security (für Mac) gesperrten URLs analysieren und entsprechende Aktionen für Websites durchführen möchten, die Sie als sicher einstufen.

6. Wenn Sie Gruppen oder Agents in der Agent-Struktur ausgewählt haben, klicken Sie auf **Speichern**, um die Einstellungen auf die ausgewählten Gruppen oder Agents anzuwenden. Wenn Sie auf das Stammsymbol ( ) geklickt haben, haben Sie folgende Optionen:

   - **Auf alle Agents anwenden**: Wendet die Einstellungen auf alle vorhandenen Agents und auf neu zu einer vorhandenen/zukünftigen Gruppe hinzukommende Agents an. Zukünftige Gruppen sind Gruppen, die bei der Konfiguration der Einstellungen noch nicht vorhanden waren.

   - **Nur auf zukünftige Gruppen anwenden**: Wendet Einstellungen nur auf Agents an, die zu zukünftigen Gruppen hinzugefügt wurden. Bei dieser Option werden die Einstellungen nicht auf neue Agents angewendet, die zu einer vorhandenen Gruppe hinzukommen.

Liste der zulässigen URLs konfigurieren

Zulässige URLs umgehen die Web-Reputation-Richtlinien. Trend Micro Security (für Mac) sperrt diese URLs nicht, selbst wenn sie laut der gültigen Web-Reputation-

Richtlinie gesperrt werden müssten. Fügen Sie URLs, die Sie als sicher einstufen, zur Liste der zulässigen URLs hinzu.

Prozedur

1. Gehen Sie zu **Administration** > **Liste der zulässigen Web Reputation URLs**.

2. Geben Sie eine URL in das Textfeld ein. Sie können an einer beliebigen Stelle der URL ein Platzhalterzeichen (*) einfügen.

   Beispiele:

   - `www.trendmicro.com/*` bedeutet, dass alle Seiten in der Domäne www.trendmicro.com zulässig sind.

   - `*.trendmicro.com/*` bedeutet, dass alle Seiten jeder untergeordneten Domäne von trendmicro.com zulässig sind.

   Sie können auch URLs eingeben, die IP-Adressen enthalten. Bei URLs mit IPv6-Adressen müssen Sie diese zwischen eckige Klammern setzen.

3. Klicken Sie auf **Hinzufügen**.

4. Klicken Sie auf das Symbol neben einer zulässigen URL, um den Eintrag zu löschen.

5. Klicken Sie auf **Speichern**.

Web-Reputation-Protokolle anzeigen

Vorbereitungen

Sie können interne Agents so konfigurieren, dass sie Web-Reputation-Protokolle an den Server senden. Dadurch können Sie die von Trend Micro Security (für Mac) gesperrten URLs analysieren und bei URLs, die Sie als sicher einstufen, eine entsprechende Aktion durchführen.

Prozedur

1. Wechseln Sie zu **Agent-Verwaltung**.
2. Klicken Sie in der Agent-Struktur auf das Stammsymbol ( ), um alle Agents oder nur bestimmte Gruppen oder Agents einzubeziehen.
3. Klicken Sie auf **Protokolle** > **Web-Reputation-Protokolle**.
4. Legen Sie die Protokollkriterien fest, und klicken Sie auf **Protokolle anzeigen**.
5. Sehen Sie die Protokolle ein. Protokolle enthalten die folgenden Informationen:
   - Datum/Uhrzeit der URL-Sperrung durch Trend Micro Security (für Mac)
   - Computer, dessen Benutzer auf die URL zugegriffen hat
   - Gesperrte URL
   - Risikostufe der URL
   - Link zum Trend Micro Web Reputation Hilfesystem, das weitere Informationen über die gesperrte URL enthält.
6. Wenn Sie das Protokoll als kommagetrennte Datei im `CSV`-Format speichern möchten, klicken Sie auf **In CSV-Datei exportieren**. Öffnen Sie die Datei, oder speichern Sie sie in einem bestimmten Verzeichnis.



Hinweis

Falls Sie eine große Anzahl an Protokollen exportieren, warten Sie bis der Export abgeschlossen ist. Wenn Sie die Seite schließen, bevor der Export abgeschlossen ist, wird die CSV-Datei nicht erzeugt.

Nächste Maßnahme

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell oder nach einem festgelegten Zeitplan. Weitere Informationen zur Verwaltung von Protokollen finden Sie unter *Protokolle verwalten auf Seite 8-5*.



Kapitel 8

Server und Agents verwalten

In diesem Kapitel werden die Verwaltung und zusätzliche Konfigurationen von Trend Micro Security (für Mac) Server und Agents erläutert.

Server und Agents aktualisieren

Die Konsole von Plug-in Manager zeigt an, wenn ein neuer Build oder eine neue Version von Trend Micro Security (für Mac) verfügbar ist.

Führen Sie das Upgrade von Server und Agents immer umgehend durch, wenn ein neuer Build oder eine neue Version verfügbar ist.

Stellen Sie vor dem Upgrade sicher, dass Server und Agents über die unter *Server-Installationsvoraussetzungen auf Seite 2-2* und *Voraussetzungen für die Installation des Agents auf Seite 4-2* beschriebenen Ressourcen verfügen.

Server aktualisieren

Vorbereitungen

Trend Micro empfiehlt die Erstellung einer Sicherungskopie der Programmdateien und Datenbank des Servers, die bei eventuellen Problemen mit dem Upgrade wiederhergestellt werden können.

- Programmdateien
  - Standardpfad:

    `C:\Programme\Trend Micro\Security Server\Addon\TMSM`

    oder

    `C:\Programme (x86)\Trend Micro\Security Server\Addon\TMSM`
  - Zu sichernde Dateien:
    - `..\apache-activemq\conf\activemq.xml`
    - `..\apache-activemq\conf\broker.pem`
    - `..\apache-activemq\conf\broker.ks`
    - `..\apache-activemq\bin\win32\wrapper.conf`
    - `..\apache-activemq\bin\win64\wrapper.conf`

- `..\ServerInfo.plist`

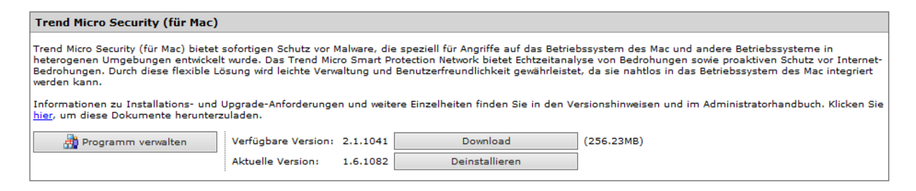
- Datenbankdateien. Weitere Informationen erhalten Sie unter *Server-Datenbank sichern auf Seite 8-8*.

Prozedur

1. Öffnen Sie die Worry-Free Business Security Webkonsole und klicken Sie im Hauptmenü auf **Voreinstellungen** > **Plug-Ins**.



2. Klicken Sie im Abschnitt **Trend Micro Security (für Mac)** auf **Download**.



   Die Größe der herunterzuladenden Datei wird neben der Schaltfläche **Download** angezeigt.

   Der Plug-in Manager lädt das Paket in den Ordner `<Installationsordner des WFBS Servers>\PCCSRV\Download\Product` herunter.

   `<Installationsordner des WFBS Servers>` ist typischerweise `C:\Programme\Trend Micro\Security Server`.

3. Verfolgen Sie den Download-Fortschritt.

Trend Micro Security (für Mac) Download

Trend Micro Security (für Mac) Version 2.1.1041 wird heruntergeladen. Bitte warten... Während des Downloads können Sie zu anderen Seiten navigieren.

Fortschritt: 3%

< Zurück

Sie können während des Downloads zu anderen Fenstern navigieren.

Wenn beim Herunterladen des Pakets Probleme auftreten, überprüfen Sie über die Worry-Free Business Security Webkonsole die Server-Update-Protokolle. Wählen Sie im Hauptmenü **Berichte** > **Protokollabfrage** aus.

4. Um das Upgrade für Trend Micro Security (für Mac) sofort durchzuführen, klicken Sie auf **Jetzt upgraden**. Wenn Sie die Installation zu einem späteren Zeitpunkt nachholen möchten, gehen Sie wie folgt vor:

a. Klicken Sie auf **Später upgraden**.

b. Öffnen Sie das Fenster Plug-in Manager.

c. Klicken Sie im Abschnitt **Trend Micro Security (für Mac)** auf **Upgrade**.

5. Verfolgen Sie den Upgrade-Fortschritt. Nach dem Upgrade wird das Fenster von Plug-in Manager neu geladen.

Agents aktualisieren

Prozedur

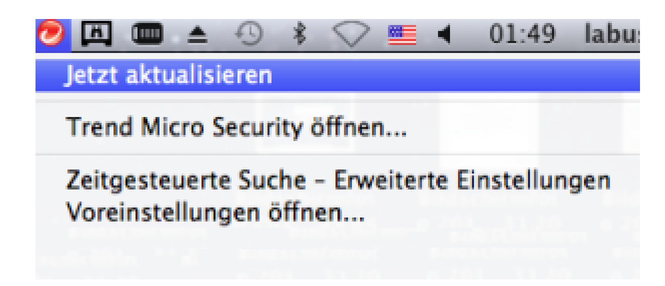
1. Führen Sie einen der folgenden Schritte durch:

- Führen Sie ein manuelles Update durch. Stellen Sie sicher, dass Sie in der Liste der Komponenten **Trend Micro Security (für Mac) Agent** auswählen.

- Wählen Sie in der Agent-Struktur die zu aktualisierenden Agents aus und klicken Sie auf **Tasks** > **Update**.

- Wenn das zeitgesteuerte Update aktiviert wurde, stellen Sie sicher, dass **Trend Micro Security (für Mac) Agent** ausgewählt wurde.

- Weisen Sie die Benutzer an, in der Agent-Konsole auf **Jetzt aktualisieren** zu klicken.



Das Upgrade wird auf allen Agents durchgeführt, die die Benachrichtigung erhalten. Auf dem Mac-Computer zeigt das Symbol für Trend Micro Security (für Mac) in der Menüleiste den laufenden Aktualisierungsvorgang an. Bis zum Abschluss des Upgrades können keine Tasks über die Konsole gestartet werden.

2. Überprüfen Sie den Upgrade-Fortschritt.

a. Klicken Sie im Hauptmenü auf **Übersicht** und gehen Sie zum Abschnitt der Agents.

b. Klicken Sie auf den Link in der Spalte **Nicht upgegradet**. Die Agent-Struktur wird geöffnet, und es werden alle Agents angezeigt, für die das Upgrade nicht durchgeführt wurde.

c. Um das Upgrade auch auf diesen durchzuführen, klicken Sie auf **Tasks** > **Update**.

Protokolle verwalten

Trend Micro Security (für Mac) führt umfangreiche Protokolle über entdeckte Sicherheitsrisiken und gesperrte URLs. Mit Hilfe dieser Protokolle können Sie die Antiviren-Richtlinien Ihres Unternehmens bewerten und Agents ermitteln, die einem höheren Infektions- oder Angriffsrisiko ausgesetzt sind.

Damit die Protokolldateien nicht zu viel Platz auf der Festplatte einnehmen, löschen Sie die Protokolle manuell oder nach einem festgelegten Zeitplan über die Webkonsole.

Prozedur

1. Gehen Sie zu **Administration** > **Protokollwartung**.
2. Wählen Sie **Zeitgesteuertes Löschen von Protokollen aktivieren**.
3. Wählen Sie aus, ob alle Protokolle gelöscht werden sollen oder nur diejenigen, die älter als eine bestimmte Anzahl an Tagen sind.
4. Geben Sie Startzeitpunkt und Zeitintervall für die Protokolllöschung an.
5. Klicken Sie auf **Speichern**.

Lizenzen verwalten

In vorherigen Versionen von Worry-Free Business Security-Servern wurde eine andere Lizenz von Trend Micro Security (für Mac) verwendet. Ab der Version Worry-Free Business Security 9 wird für den Worry-Free Business Security-Server und Trend Micro Security (für Mac) dieselbe Lizenz verwendet. Bei einer entsprechenden Abfrage ruft Trend Micro Security (für Mac) die Worry-Free Business Security-Serverlizenz automatisch ab.

Der Status der Produktlizenz bestimmt, welche Funktionen den Benutzern zur Verfügung stehen. Genaue Angaben finden Sie in der nachfolgenden Tabelle.

LIZENZTYP UND STATUS	FUNKTIONEN			
	ECHTZEITSUCHE	MANUELLE/ ZEITGESTEUERTE SUCHE	WEB REPUTATION	PATTERN-UPDATE
Vollversion und Aktiviert	Aktiviert	Aktiviert	Aktiviert	Aktiviert
Testversion (Demo) und aktiviert	Aktiviert	Aktiviert	Aktiviert	Aktiviert
Vollversion und abgelaufen	Aktiviert	Aktiviert	Deaktiviert	Deaktiviert

Lizenztyp und Status	Funktionen			
	Echtzeitsuche	Manuelle/ zeitgesteuerte Suche	Web Reputation	Pattern-Update
Testversion und abgelaufen	Deaktiviert	Deaktiviert	Deaktiviert	Deaktiviert
Nicht aktiviert	Deaktiviert	Deaktiviert	Deaktiviert	Deaktiviert



Hinweis

Wenn der Server nur eine IPv6-Adresse aufweist, lesen Sie den Abschnitt über die Einschränkungen bei IPv6 für Lizenzaktualisierungen in *Einschränkungen eines reinen IPv6-Servers auf Seite A-3*.

Prozedur

1. Gehen Sie zu **Administration** > **Produktlizenz** .

2. Informationen zur Produktlizenz anzeigen. Um aktuelle Lizenzinformationen zu erhalten, klicken Sie auf **Informationen aktualisieren**.

   Der Abschnitt **Lizenzinformationen** enthält folgende Informationen:

   - **Status**: Zeigt entweder „Aktiviert“ oder „Abgelaufen“ an.
   - **Version**: Zeigt entweder „Vollversion“ oder „Testversion“ an. Wenn Sie die Testversion verwenden, können Sie jederzeit auf die Vollversion upgraden. Um Upgrade-Anweisungen zu erhalten, klicken Sie auf **Hinweise für das Upgrade der Lizenz anzeigen**.
   - **Arbeitsplätze**: Die maximal zulässige Anzahl von Agent-Installationen, die die Lizenz unterstützt
   - **Lizenz läuft ab am**: Das Ablaufdatum der Lizenz
   - **Aktivierungscode**: Der für die Aktivierung der Lizenz verwendete Code.

Server-Datenbank sichern

Prozedur

1. Halten Sie die folgenden Dienste über die Microsoft Management Console an:
   - **ActiveMQ für Trend Micro Security**
   - **Trend Micro Security für (Mac)**
2. Öffnen Sie SQL Server Management Studio (z. B. über **Windows Start-Menü** > **Programme** > **Microsoft SQL Server {Version}** > **SQL Server Management Studio**.
3. Suchen Sie nach `db_TMSM` und verwenden Sie dann die **Sicherung**sfunktion in SQL Server Management Studio, um die Datenbankdateien zu sichern.

   Details finden Sie in der SQL Server Management Studio-Dokumentation.
4. Starten Sie die angehaltenen Dienste.

Serverdatenbank wiederherstellen

Vorbereitungen

Bereiten Sie die Sicherung der während der Sicherung erstellten Datenbankdateien vor. Weitere Informationen finden Sie unter *Server-Datenbank sichern auf Seite 8-8*.

Prozedur

1. Halten Sie die folgenden Dienste über die Microsoft Management Console an:
   - **ActiveMQ für Trend Micro Security**
   - **Trend Micro Security für (Mac)**

2. Öffnen Sie SQL Server Management Studio (z. B. über **Windows Start-Menü** > **Programme** > **Microsoft SQL Server {Version}** > **SQL Server Management Studio**.

3. Suchen Sie `db_TMSM` und verwenden Sie die Option **Trennen** (Detach) in SQL Server Management Studio zum Abtrennen der aktuellen Datenbankdateien.

   Details finden Sie in der SQL Server Management Studio-Dokumentation.

4. Hängen Sie die gesicherten Datenbankdateien mit der Option **Anhängen** (Attach) an.

5. Starten Sie die angehaltenen Dienste.

Agent-Server-Kommunikationseinstellungen konfigurieren

Agents identifizieren den Server, der sie verwaltet, anhand des Servernamens oder der IPv4/IPv6-Adresse. Während der Installation des Trend Micro Security (für Mac) Servers ermittelt das Installationsprogramm die IP-Adressen des Servers. Diese werden dann im Fenster Agent/Server-Kommunikation in der Webkonsole angezeigt.

Der Server kommuniziert mit Agents über den Listening-Port (Voreinstellung: 61617).

Anmerkungen und Erinnerungen:

- Wenn Sie eine andere Portnummer angeben, vergewissern Sie sich, dass diese noch nicht durch eine andere Anwendung genutzt wird, um Konflikte und Probleme bei der Agent/Server-Kommunikation zu vermeiden.

- Falls auf dem Server eine Firewall verwendet wird, stellen Sie sicher, dass sie nicht den Listening-Port für die Agent/Server-Kommunikation blockiert. Falls auf dem Computer beispielsweise die Worry-Free Business Security Agent-Firewall aktiviert wurde, fügen Sie eine Richtlinienausnahme hinzu, die eingehenden und ausgehenden Datenverkehr über den Listening-Port zulässt.

- Sie können Agents so konfigurieren, dass sie sich über einen Proxy-Server mit dem Server verbinden. Für gewöhnlich ist für die Agent/Server-Kommunikation innerhalb eines Unternehmensnetzwerks kein Proxy-Server notwendig.

- Wenn Sie planen, alle vorhandenen Servernamen und IPv4/IPv6-Adressen zu aktualisieren oder zu ersetzen oder den Listening-Port oder Proxy-Einstellungen zu ändern, tun Sie das vor der Installation von Agents. Falls Sie Agents installiert haben und Einstellungen ändern, verlieren die Agents die Verbindung zum Server, und die einzige Möglichkeit, die Verbindung wieder aufzubauen, besteht darin, die Agents erneut zu verteilen.

Prozedur

1. Wechseln Sie zu **Administration** > **Kommunikation zwischen Agent und Server**.

2. Geben Sie den Servernamen oder die IPv4/IPv6-Adresse(n) und den Listening-Port ein.



Hinweis

Wenn im Feld **Name (oder IP-Adresse) des Servers** mehrere Einträge vorhanden sind, wählt der Agent nach dem Zufallsprinzip einen Eintrag aus. Stellen Sie sicher, dass die Verbindung zwischen Agent und Server über alle Einträge hergestellt werden kann.

3. Wählen Sie aus, ob sich Agents über einen Proxy-Server mit dem Server verbinden.

   a. Wählen Sie das Proxy-Server-Protokoll.

   b. Geben Sie den Namen des Proxy-Servers oder seine IPv4/IPv6-Adresse und die Portnummer ein.

   c. Falls der Proxy-Server einen Benutzernamen und ein Kennwort erfordert, geben Sie diese in die dafür vorgesehenen Textfelder ein.

4. Klicken Sie auf **Speichern**.

5. Wenn Sie aufgefordert werden, die Trend Micro Security (für Mac) Dienste neu zu starten, damit die Einstellungen wirksam werden, führen Sie die folgenden Schritte aus:

   a. Wechseln Sie zum <*Server-Installationsordner*>.

   b. Doppelklicken Sie auf `restart_TMSM.bat`.

c. Warten Sie, bis alle Dienste neu gestartet sind.

Agent-Symbole

Symbole in der Task-Leiste des Mac-Computers zeigen den Status des Agents an und den Task, der gerade ausgeführt wird.

Symbol	Farbe	Beschreibung
	Rot	Der Agent ist gestartet und wird ausgeführt und ist mit dem übergeordneten Server verbunden. Außerdem gilt Folgendes: • Die Produktlizenz wurde aktiviert. • Die Produktlizenz (Voll- oder Testversion) wurde aktiviert, ist aber abgelaufen. Einige Agent-Funktionen sind nicht verfügbar, wenn die Lizenz abgelaufen ist. Weitere Informationen finden Sie unter *Lizenzen verwalten auf Seite 8-6*.
	Grau	Der Agent ist gestartet und wird ausgeführt, ist aber nicht mit dem übergeordneten Server verbunden.
	Rot	Der Agent sucht gerade nach Sicherheitsrisiken und ist mit dem übergeordneten Server verbunden.
	Grau	Der Agent sucht gerade nach Sicherheitsrisiken, ist aber nicht mit dem übergeordneten Server verbunden. Werden während der Suche Sicherheitsrisiken entdeckt, wird das Suchergebnis erst an den Server gesendet, wenn die Verbindung wiederhergestellt ist.
	Rot	Der Agent aktualisiert Komponenten über den übergeordneten Server.

SYMBOL	FARBE	BESCHREIBUNG
	Grau	Der Agent aktualisiert Komponenten über den Trend Micro ActiveUpdate Server, weil keine Verbindung zum übergeordneten Server hergestellt werden kann.
	Grau	Die Anzeige dieses Symbol bedeutet: • Der Agent wurde beim übergeordneten Server registriert, aber die Produktlizenz wurde nicht aktiviert. Einige Agent-Funktionen sind nicht verfügbar, wenn die Lizenz nicht aktiviert wurde. Weitere Informationen finden Sie unter *Lizenzen verwalten auf Seite 8-6*. • Der Agent wurde nicht beim übergeordneten Server registriert. Die Produktlizenz kann aktiviert oder nicht aktiviert sein. Wenn ein Agent nicht beim übergeordneten Server registriert wurde: • Die Echtzeitsuche ist aktiviert, aber die Aktion bei Sicherheitsrisiken ist immer "Übergehen". • Manuelle Suche, zeitgesteuerte Suche, Web Reputation und Pattern-Updates sind deaktiviert. • Der Agent wurde beim übergeordneten Server registriert. Die Produktlizenz ist für eine Testversion des Produkts gültig und wurde aktiviert. Die Lizenz für die Testversion ist jedoch abgelaufen. Einige Agent-Funktionen sind nicht verfügbar, wenn die Lizenz abgelaufen ist. Weitere Informationen finden Sie unter *Lizenzen verwalten auf Seite 8-6*.



Kapitel 9

Hilfe anzeigen

Dieses Kapitel beschreibt die Behebung von Problemen, die auftreten können, und die Kontaktaufnahme mit dem Support.

Fehlerbehebung

Zugriff auf die Webkonsole

Problem:

Es kann nicht auf die Webkonsole zugegriffen werden.

Prozedur

1. Überprüfen Sie, ob der Computer die Voraussetzungen zum Installieren und Ausführen von Trend Micro Security (für Mac) Server erfüllt. Weitere Informationen finden Sie unter *Server-Installationsvoraussetzungen auf Seite 2-2*.

2. Überprüfen Sie, ob die folgenden Dienste gestartet sind:

    - **ActiveMQ für Trend Micro Security**
    - **Trend Micro Plug-in Manager**
    - **SQL Server (TMSM)**
    - **Trend Micro Security für (Mac)**

3. Durchsuchen Sie die Debug-Protokolle. Durchsuchen Sie die Protokolle mit Hilfe der Suchfunktion nach den Schlüsselwörtern ‚Fehler' oder ‚Fehlgeschlagen'.

    - **Installationsprotokolle**: `C:\TMSM*.log`
    - **Allgemeine Debug-Protokolle**: <*Server-Installationsordner*>`\debug.log`
    - **Worry-Free Business Security Debug-Protokolle**: `C:\Programme \Trend Micro\Security Server\PCCSRV\Log\ofcdebug.log`

        a. Aktivieren Sie die Debug-Protokollierung, wenn die Datei nicht vorhanden ist. Klicken Sie im Banner der Worry-Free Business Security Webkonsole auf „M" in „Trend Micro", geben Sie die Einstellungen für die Debug-Protokolle an, und klicken Sie auf **Speichern**.

        b. Wiederholen Sie die Schritte, die zum Problem mit dem Zugriff auf die Webkonsole geführt haben.

c. Durchsuchen Sie die Debug-Protokolle.

4. Überprüfen Sie die Registrierungsschlüssel für Trend Micro Security (für Mac). Gehen Sie dazu zu `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMSM`.

5. Überprüfen Sie die Datenbankdateien und Registrierungsschlüssel.

   a. Überprüfen Sie, ob in `C:\Programme\Microsoft SQL Server\MSSQL.x\MSSQL\Data\` die folgenden Dateien vorhanden sind:

      - `db_TMSM.mdf`
      - `db_TMSM_log.LDF`

   b. Überprüfen Sie, ob die Datenbankinstanz für Trend Micro Security (für Mac) im Registrierungsschlüssel von Microsoft SQL Server vorhanden ist:

      - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\Instance Names`
      - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.x\MSSQLServer\CurrentVersion`

6. Senden Sie die folgenden Informationen an Trend Micro:

   - Registrierungsdateien

     a. Gehen Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL server\TMSM`.

     b. Klicken Sie auf **Datei** > **Exportieren** und speichern Sie den Registrierungsschlüssel in einer `.reg`-Datei.

   - Angaben zum Server

     - Version des verwendeten Betriebssystems
     - Verfügbarer Speicherplatz
     - Verfügbarer Arbeitsspeicher
     - Informationen darüber, ob andere Plug-in-Programme installiert sind, z. B. Intrusion Defense Firewall.

7. Starten Sie die Dienste für Trend Micro Security (für Mac) neu.

a. Wechseln Sie zum <*Server-Installationsordner*>.

b. Doppelklicken Sie auf `restart_TMSM.bat`.

c. Warten Sie, bis alle Dienste neu gestartet sind.

8. Der Dienst Trend Micro Security (für Mac) sollte immer ausgeführt werden. Sollte dieser Dienst nicht aktiv sein, liegt möglicherweise ein Problem mit dem Dienst ‚ActiveMQ' vor.

a. Erstellen Sie eine Sicherheitskopie der ActiveMQ-Daten, die sich in `C:\Programme\Trend Micro\Security Server\Addon\TMSM\apache-activemq\data\*.* befinden`.

b. Löschen Sie die ActiveMQ-Daten.

c. Versuchen Sie, den Dienst für Trend Micro Security (für Mac) durch Doppelklicken auf `restart_TMSM.bat` neu zu starten.

d. Versuchen Sie erneut, auf die Webkonsole zuzugreifen, um zu überprüfen, ob das Problem gelöst wurde.

Server-Deinstallation

Problem:

Die folgende Meldung wird angezeigt:

```
Unable to uninstall the plug-in program. The uninstallation
command for the plug-in program is missing in the registry key.
```

Prozedur

1. Öffnen Sie den Registrierungseditor und gehen Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`.

2. Setzen Sie den Wert auf `1.0.1000` zurück.

3. Löschen Sie den Registrierungsschlüssel des Plug-in-Programms, z. B. `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_xxxx`.

4. Starten Sie den Trend Micro Plug-in Manager Service neu.

5. Laden Sie das Plug-in-Programm herunter, installieren Sie es, und deinstallieren Sie es anschließend.

Agent-Installation

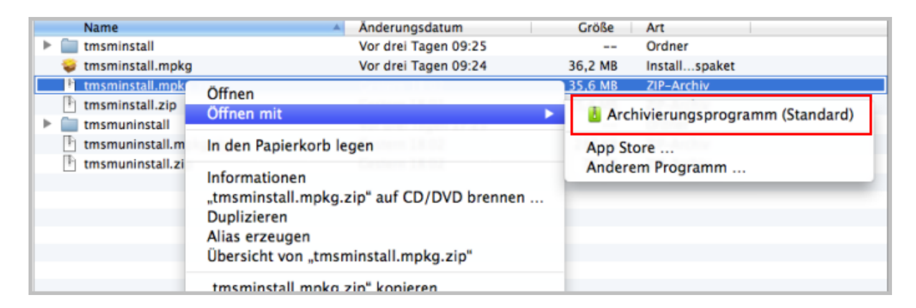
Problem:

Die Installation ist fehlgeschlagen. Das Installationspaket (`tmsminstall.zip` oder `tmsminstall.mpkg.zip`) wurde mit einem nicht im Mac-Computer integrierten Archivierungsprogramm oder einem nicht unterstützten Befehl (z. B. `unzip`) aus einem Befehlszeilenprogramm gestartet, wodurch der entpackte Ordner (`tmsminstall`) oder die entpackte Datei (`tmsminstall.mpkg`) beschädigt wurden.

Prozedur

1. Entfernen Sie den entpackten Order (`tmsminstall`) bzw. die entpackte Datei (`tmsminstall.mpkg`).

2. Starten Sie das Installationspaket mit einem integrierten Archivierungsprogramm.



Mit dem folgenden Befehl kann das Paket auch von der Befehlszeile ausgeführt werden:

- Wenn das Paket `tmsminstall.zip` lautet:

  ```
  ditto -xk <tmsminstall.zip file path> <destination
  folder>
  ```

  Zum Beispiel:

  ```
  ditto -xk users/mac/Desktop/tmsminstall.zip users/mac/
  Desktop
  ```

- Wenn das Paket `tmsminstall.mpkg.zip` lautet:

  ```
  ditto -xk <tmsminstall.mpkg.zip file path> <destination
  folder>
  ```

  Zum Beispiel:

  ```
  ditto -xk users/mac/Desktop/tmsminstall.mpkg.zip
  users/mac/Desktop
  ```

Allgemeiner Agent-Fehler

Problem:

Im Agent ist ein Fehler oder ein Problem aufgetreten.

Prozedur

1. Öffnen Sie <*Agent-Installationsordner*>`/Tools` und starten Sie Trend Micro Debug Manager.
2. Folgen Sie den Programmanweisungen, um die Informationen zu ermitteln.



Warnung!

Das Programm funktioniert nicht, wenn es in einen anderen Ordner auf dem Mac-Computer verschoben wurde. Falls es verschoben wurde, deinstallieren Sie den Trend Micro Security (für Mac) Agent und installieren Sie ihn neu.

Wenn das Programm in einen anderen Ordner kopiert wurde, entfernen Sie die Kopie und starten Sie das Programm aus dem ursprünglichen Ordner.

Die Knowledge Base von Trend Micro

Die Knowledge Base befindet sich auf der Website von Trend Micro. Sie enthält die aktuellsten Antworten auf Fragen zu den Produkten. Wenn Sie in der Produktdokumentation keine Antwort auf Ihre Frage finden, können Sie die Frage auch über die Knowledge Base an das Supportteam richten. Zugriff auf die Knowledge Base erhalten Sie unter:

http://esupport.trendmicro.com/en-us/business/default.aspx

Trend Micro aktualisiert die Einträge in der Knowledge Base regelmäßig und erweitert sie täglich um neue Lösungen. Wenn Sie keine Lösung für Ihr Problem finden, können Sie dieses auch in einer E-Mail schildern und direkt an einen Support-Mitarbeiter von Trend Micro senden, der das Problem untersucht und Ihnen schnellstmöglich weiterhilft.

Mit dem technischen Support Verbindung aufnehmen

Trend Micro bietet allen registrierten Benutzern technischen Support, Pattern-Downloads und Programm-Updates für die Dauer eines (1) Jahres. Nach Ablauf dieser Frist muss der Wartungsvertrag verlängert werden. Setzen Sie sich mit uns in Verbindung, wenn Sie Hilfe benötigen oder eine Frage haben. Wir freuen uns ebenso über Ihre Anregungen.

Support-Niederlassungen weltweit:

http://esupport.trendmicro.com/en-us/default.aspx?locale=de_de

Produktdokumentation von Trend Micro

http://docs.trendmicro.com/de-de/home.aspx

Support-Anfrage beschleunigen

Bei der Kontaktaufnahme mit Trend Micro sollten Sie folgende Informationen bereithalten:

- Version von Microsoft Windows und des Service Packs
- Art des Netzwerks
- Marke und Modell des Computers sowie zusätzliche Hardware, die an den Computer angeschlossen ist
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen
- Schritte, um das Problem nachvollziehen zu können

Kontaktaufnahme mit Trend Micro

In Deutschland erreichen Sie unsere Trend Micro Vetriebspartner telefonisch, per Fax oder E-Mail:

Adresse	Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Tel.:	+49 (0) 811 88990-700
Fax:	+4981188990799
Website	http://www.trendmicro.com

E-Mail-Adresse	support@trendmicro.com

- Support-Niederlassungen weltweit:

  http://www.trendmicro.de/ueber-uns/kontakt/index.html

- Produktdokumentation von Trend Micro

  http://www.trendmicro.com/download/emea/?lng=de

Sicherheitsinformationen

Umfassende Sicherheitsinformationen finden Sie auf der Trend Micro Website.

- Liste mit Viren und bösartigen mobilen Codes, die zum jeweiligen Zeitpunkt im Umlauf und aktiv sind
- Falschmeldungen (Hoaxes)
- Beratung zu Internet-Bedrohungen
- Wöchentlicher Virenbericht
- Virenenzyklopädie, die eine ausführliche Liste von Namen und Symptomen bekannter Viren und bösartigen mobilen Codes enthält

  http://about-threats.trendmicro.com/threatencyclopedia.aspx

- Glossar

TrendLabs

TrendLabs℠ ist das globale Netzwerk für Antiviren-Forschung und Support von Trend Micro. Auf drei Kontinenten und mit über 250 Virenforschern und -experten, die rund um die Uhr im Einsatz sind, stellt TrendLabs Service und Support für Sie und alle Trend Micro Kunden bereit.

Nach dem Kauf eines Trend Micro Produkts stehen Ihnen folgende Service-Leistungen zur Verfügung:

- Regelmäßige Viren-Pattern-Updates für alle bekannten "In-the-zoo"- und "In-the-wild"-Computerviren und bösartigen Codes
- Notfall-Support bei Virenausbruch
- E-Mail-Kontakt mit Antiviren-Technikern
- Knowledge Base, die Online-Datenbank von Trend Micro mit Informationen über bekannte Probleme

TrendLabs besitzt die ISO-9002-Qualitätssicherungszertifizierung.

Anregungen und Kritik

Das Trend Micro Team ist stets bemüht, die Dokumentationen zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder einem anderen Dokument von Trend Micro besuchen Sie diese Website:

http://www.trendmicro.com/download/documentation/rating.asp



Anhang A

IPv6-Unterstützung in Trend Micro Security (für Mac)

Dieser Anhang enthält kritische Informationen für die Bereitstellung von Trend Micro Security (für Mac) in einer Umgebung mit IPv6-Adressierung. Er bietet wichtige Hinweise zum Ausmaß der IPv6-Unterstützung in Trend Micro Security (für Mac).

Trend Micro geht davon aus, dass der Leser über die erforderlichen Kenntnisse der Konzepte von IPv6 und der Arbeitsschritte verfügt, die zur Einrichtung eines Netzwerks mit IPv6-Adressierung benötigt werden.

IPv6-Unterstützung für Trend Micro Security (für Mac) Server und Agents

IPv6-Unterstützung in Trend Micro Security (für Mac) ist ab Version 2.0 verfügbar. Frühere Versionen von Trend Micro Security (für Mac) bieten keine Unterstützung für IPv6-Adressen. Die IPv6-Unterstützung wird nach der Installation oder dem Upgrade der IPv6-kompatiblen Trend Micro Security (für Mac) Server und Agents automatisch aktiviert.

IPv6-Voraussetzungen für Trend Micro Security (für Mac) Server

Trend Micro Security (für Mac) Server muss zusammen mit einer Version von Worry-Free Business Security Server installiert werden, die IPv6 unterstützt.

IPv6-Unterstützung in Worry-Free Business Security ist ab Version 8.0 verfügbar. Frühere Worry-Free Business Security Versionen, die mit Trend Micro Security (für Mac) kompatibel sind (siehe *Server-Installationsvoraussetzungen auf Seite 2-2*), bieten keine Unterstützung für IPv6-Adressen.

Details zur IPv6-Unterstützung finden Sie in der Dokumentation zu Worry-Free Business Security 9.0 oder höher.

IPv6-Voraussetzungen für Trend Micro Security (für Mac) Agent

Alle Mac OS X-Versionen, die vom Trend Micro Security (für Mac) Agent unterstützt werden, bieten auch Unterstützung für IPv6.

Es empfiehlt sich, für den Agent sowohl eine IPv4- als auch eine IPv6-Adresse anzugeben, da bestimmte Entitäten, mit denen er sich verbinden soll, nur IPv4-Adressen unterstützen.

Einschränkungen eines reinen IPv6-Servers

Die folgende Tabelle enthält eine Liste der Einschränkungen für Trend Micro Security (für Mac) Server mit ausschließlich einer IPv6-Adresse.

TABELLE A-1. Einschränkungen eines reinen IPv6-Servers

ELEMENT	EINSCHRÄNKUNG
Agent-Verwaltung	Reine IPv4-Agents können nicht über einen reinen IPv6-Server verwaltet werden.
Updates und zentrale Verwaltung	Reine IPv6-Server können nicht aus reinen IPv4-Aktualisierungsquellen aktualisiert werden oder an reine IPv4-Produkte für zentrale Verwaltung wie die folgenden melden: • Trend Micro ActiveUpdate Server • Jede reine IPv4-Quelle für benutzerdefinierte Updates
Produktregistrierung, -aktivierung und -verlängerung	Reine IPv6-Server können keine Verbindung mit dem Trend Micro Online-Registrierungsserver herstellen, um das Produkt zu registrieren, die Lizenz abzurufen und die Lizenz zu aktivieren oder zu verlängern.
Proxyverbindung	Reine IPv6-Server können keine Verbindungen über reine IPv4-Proxyserver herstellen.

Die meisten dieser Einschränkungen können mit Hilfe eines Dualstapel-Proxyservers umgangen werden, der IPv4- in IPv6-Adressen und umgekehrt umwandeln kann (z. B. DeleGate). Setzen Sie den Proxyserver zwischen den Trend Micro Security (für Mac) Server und die Entitäten, mit denen er zusammenarbeitet.

Einschränkungen eines reinen IPv6-Agents

Die folgende Tabelle enthält eine Liste der Einschränkungen für Agents mit ausschließlich einer IPv6-Adresse.

TABELLE A-2. Einschränkungen eines reinen IPv6-Agents

ELEMENT	EINSCHRÄNKUNG
Übergeordneter Server	Reine IPv6-Agents können nicht über einen reinen IPv4-Server verwaltet werden.
Updates	Reine IPv6-Agents können nicht aus reinen IPv4-Aktualisierungsquellen wie die folgenden aktualisiert werden: • Trend Micro ActiveUpdate Server • Reiner IPv4-Trend Micro Security (für Mac) Server
Web-Reputation-Abfragen	Reine IPv6-Agents können keine Web-Reputation-Abfragen an das Trend Micro Smart Protection Network senden.
Proxyverbindung	Reine IPv6-Agents können keine Verbindungen über reine IPv4-Proxyserver herstellen.
Bereitstellung von Agents	Apple Remote Desktop ist nicht in der Lage, reinen IPv6-Computern Agents bereitzustellen, da diese Computer immer als offline angezeigt werden.

Die meisten dieser Einschränkungen können mit Hilfe eines Dualstapel-Proxyservers umgangen werden, der IPv4- in IPv6-Adressen und umgekehrt umwandeln kann (z. B. DeleGate). Setzen Sie den Proxyserver zwischen die Agents und die Entitäten, mit denen sie sich verbinden sollen.

IPv6-Adressen konfigurieren

In der Webkonsole können Sie eine IPv6-Adresse oder einen Bereich von IPv6-Adressen konfigurieren. Im Folgenden erhalten Sie einige Richtlinien für die Konfiguration.

- Trend Micro Security (für Mac) akzeptiert die Standarddarstellung von IPv6-Adressen.

  Zum Beispiel:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

`2001:db7:85a3::8a2e:370:7334`

`::ffff:192.0.2.128`

- Trend Micro Security (für Mac) akzeptiert ebenso verbindungslokale IPv6-Adressen wie:

  `fe80::210:5aff:feaa:20a2`



Warnung!

Seien Sie vorsichtig, wenn Sie verbindungslokale IPv6-Adressen angeben, da sie unter bestimmten Umständen nicht wie erwartet funktionieren könnten, auch wenn Trend Micro Security (für Mac) sie akzeptiert. Beispielsweise können Agents nicht aus einer Aktualisierungsquelle in einem anderen Netzwerksegment aktualisiert werden, wenn dieses durch eine verbindungslokale IPv6-Adresse angegeben wird.

- IPv6-Adressen, die Teil einer URL sind, müssen zwischen eckige Klammern gesetzt werden.
- Bei IPv6-Adressbereichen ist üblicherweise ein Präfix und eine Präfixlänge erforderlich.

Fenster mit Anzeige von IP-Adressen

In der Agent-Struktur werden die IPv6-Adressen der Agents in der Spalte **IPv6-Adresse** angezeigt.



Anhang B

Produktterminologie und -begriffe

Die in diesem Anhang enthaltenen Elemente bieten weitere Informationen zu Trend Micro Produkten und Technologien.

IntelliScan

IntelliScan ist ein Verfahren, um festzustellen, welche Dateien durchsucht werden müssen. Bei ausführbaren Dateien wie beispielsweise `.exe` wird der ursprüngliche Dateityp (True File Type) über den Dateiinhalt bestimmt. Bei nicht ausführbaren Dateien wie beispielsweise `.txt` wird der ursprüngliche Dateityp über den Datei-Header bestimmt.

Die Verwendung von IntelliScan bietet die folgenden Vorteile:

- Leistungsoptimierung: IntelliScan beeinträchtigt keine Anwendungen auf dem Endpunkt, da nur minimale Systemressourcen benötigt werden.
- Kürzere Virensuchzeiten: Da IntelliScan die „True File Type“-Erkennung verwendet, werden nur Dateien durchsucht, für die ein Infektionsrisiko besteht. Die Suchzeit verkürzt sich gegenüber der Suche in allen Dateien erheblich.

Dateien, die nicht gesäubert werden können

Die Viren-Scan-Engine kann folgende Dateien nicht säubern:

Nicht zu säubernde Datei	Erklärung und Lösung
Mit Würmern infizierte Dateien	Ein Computerwurm ist ein eigenständiges Programm (oder eine Gruppe von Programmen), das funktionsfähige Kopien von sich selbst oder seinen Segmenten an andere Computer verteilen kann. Würmer verbreiten sich normalerweise über Netzwerkverbindungen oder E-Mail-Anhänge. Würmer sind eigenständige Programme und können deshalb nicht gesäubert werden. **Lösung**: Trend Micro empfiehlt, Würmer zu löschen.
Infizierte, schreibgeschützte Dateien	**Lösung**: Heben Sie den Schreibschutz auf, damit der Trend Micro Security (für Mac) Agent die Datei säubern kann.

Nicht zu säubernde Datei	Erklärung und Lösung
Kennwortgeschützte Dateien	Schließt kennwortgeschützte Dateien und komprimierte Dateien ein. **Lösung**: Heben Sie den Kennwortschutz auf, damit der Trend Micro Security (für Mac) Agent diese Dateien säubern kann.
Sicherungsdateien	Bei Dateien mit den Erweiterungen RB0~RB9 handelt es sich um Sicherungskopien infizierter Dateien. Trend Micro Security (für Mac) erstellt diese Kopien für den Fall, dass der Virus/die Malware die infizierte Datei beim Säubern beschädigt. **Lösung**: Wenn der Trend Micro Security (für Mac) Agent die infizierte Datei erfolgreich säubert, muss die Sicherungskopie nicht aufbewahrt werden. Wenn Ihr Computer fehlerfrei funktioniert, können Sie die Kopie löschen.



Stichwortverzeichnis



TREND MICRO INCORPORATED

Trend Micro Deutschland GmbH Zeppelinstraβe 1 Hallbergmoos, Bayern 85399 Deutschland

Tel.: +49 (0) 811 88990-700 Fax: +4981188990799 info@trendmicro.com

www.trendmicro.com

Element-Code: TSGM26484/140925